

THEFT



PREVENTION



BERSERKER

BOOKS



Contents

INTRODUCTION	1
1 TACTICS IN ILLEGAL ENTRY	5
Target Reconnaissance and Initial Planning	
Overt Entry	
Covert Entry	
2 LOCKS AND LOCK PICKING	19
Warded Locks	
Lever Tumbler Locks	
Disc Tumbler Locks	
Pin Tumbler Cylinder Locks	
Tubular Cylinder Locks	
Vehicle Locks	
Magnetic Locks	
Simple Suitcase Locks	
Safes and Combination Locks	
Padlocks	
Master Key Systems	
3 IMPROVISING LOCK-PICKING TOOLS	63

4 OTHER MEANS OF ILLEGAL ENTRY

73

- Window Entry
- Transom Entry, Doors, and Door Chains
- File Cabinets and Desk Drawers
- Vehicle Doors, Windows, and Trunks

5 METHODS OF FORCED ENTRY

91

- Doors
- Windows
- Security Bars
- Safe Cracking

6 ALARM SYSTEMS, SENSORS, AND HOW TO AVOID THEM 109

- Control Units
- Warning Devices
- Remote Signaling Systems and Automatic Dialers
- Access and Exit Control Systems
- Lock Switches Built into Standard, Mechanical
Mortise Locks
- Power Supply and Batteries
- Wiring
- Wireless Systems

7 ALARM SENSORS

141

- Magnetic Reed Switches and Wire Contact Systems
- Window Foil
- Windowpane-Mounted Glass Breakage Detectors
- Vibration Detectors and Inertia Sensors
- Infrasound Detectors
- Field Effect Sensors
- Sound Detectors and Heat Detectors
- Pressure Mats, Plunger Switches, and Contact Strips

Ionization Detectors
Photoelectric Cells and Invisible Beam Detectors
Passive Infrared Detectors
Microwave Motion Detectors
Ultrasonic Motion Detectors
Visible Light Detectors
Video Detectors
Barrier Sensors and Analyzers

8 OTHER TYPES OF ALARM SYSTEMS 177

Deliberately Activated Alarm Systems and Personal
Attack Alarms
Car Alarm Systems
Shoplifter Detection Systems
Fire Alarm Systems

9 ENTRY TRICKS 197

Note

As this book was originally written in Europe, all measurements follow the international metric system. No measurements are absolute, however, as they always must be adapted to the measurements of the actual lock or device you are working on.

1 millimeter = 0.039 in.

1 centimeter = 0.39 in.

1 meter = 39.37 in.

10 meters = 32.81 ft.

Tactics in Illegal Entry

The outcome of an entry operation depends on two important factors: tactics and techniques. The chosen tactics determine how to conduct the entry as an operation and how to avoid being detected or caught. The techniques are the actual methods used for bypassing locks, doors, and other obstacles, such as alarm systems. This chapter will concentrate on tactics, while the following chapters will detail the actual techniques in use.

The first thing to do when planning an entry operation is to reconnoiter the target (i.e., the actual building or installation to be entered) and the area around it. This is the reconnaissance phase.

TARGET RECONNAISSANCE AND INITIAL PLANNING

First of all, the following factors about the target must be determined.

1) Protection:

- number of guards, if any
- location of guards at particular times
- their equipment and armament
- technical details on alarm and controlled-entry systems, if any

2) Layout:

- number and locations of entrances and exits (both ordinary and emergency exits) and hallways or stairways suitable for a quick escape (and possibly windows, rooftops, and sewers—even chutes in an emergency)
- location of important offices or other rooms of importance
- method of smuggling entry team and equipment into the building if ordinary access is denied
- possibilities of temporarily cutting off the entire building from the telephone network and other ways of preventing communication with the outside, for instance, with cellular telephones or radio transmitters

3) Personnel:

- number of staff in the building during and after ordinary office hours
- their location at particular times

4) Timing:

- when the target is most vulnerable
- if there are any outside factors which will influence the accomplishment of the entry operation

Most targets are most vulnerable between 2 A.M. and 4 A.M., as most people are asleep at that time, and any security guards tend to be sleepy and therefore less vigilant during these hours. It is, however, vital to check the guards, as different individuals keep different habits.

There are many types of outside factors which might affect the mission. If breaking into a government building or an industrial complex, especially one of military importance, consider, for instance, the possibility of a surprise inspection by a senior official surrounded by a large number of guards. This is perhaps a worst-case scenario, but other things may also affect the operation, such as the sud-

den removal or installation of important machines. Such work, and also regular maintenance work, is often performed outside ordinary office hours so as not to delay the regular work.

The vicinity of the target building must also be carefully reconnoitered. Suitable escape routes must be prepared, both for use after a successful entry and in the case of failure. If several operatives are available, it is advisable to organize an outer security ring around the target during the actual entry. The members of the outer security ring will be positioned some distance away from the actual target. They will observe access routes and warn of the approach of police or enemies, either on foot or in vehicles. Warnings are generally passed on by radio, preferably through the use of innocent-sounding code words, so that the transmission cannot be identified if it is monitored.

One way of obtaining information on the tenants of a particular building is to play the role of a private detective. Such detectives sometimes pry into the comings and goings of tenants, especially in divorce cases. This is more common in certain countries than in others, however, so operatives should be careful when assuming this role.

Another way of getting information on tenants is to go through their trash. An office especially yields a surprisingly large amount of trash, most of it in the form of discarded documents. This can give much valuable information. This method is highly useful in determining whether an entry operation is called for or not.

Torn or burned scraps of letters might be found that will indicate whether an entry and a search will be fruitful or not. Burned or dirty pieces of paper can be read through the use of special equipment. It is not unheard of for a businessman to very carefully destroy his important letters, while his secretary simply discards her stenographic notebooks in the wastepaper basket, where they are found by a delighted operative who is trying to piece together the businessman's activities.

At this stage, it is also prudent that every member of the entry team familiarize himself with the appearance of

everybody working in the building at the proposed time of entry, as well as that of every resident or employee of the target apartment or office. In this way, the members of the outer security ring can easily recognize any potential threat and sound the alarm in time to warn the entry team if somebody is approaching the target area.

This familiarization process has frequently been accomplished by sending the members of the team to the building in daytime, dressed as cleaners, maintenance crew, or repairmen. They can then spend plenty of time fixing some minor problem or painting a wall or another object, and at the same time get a close look at the entire staff of the building. One good way of identifying everybody is to litter the floor with tools and then warn every passer-by not to stumble on them. Of course, a sufficient cover is required for this kind of job, including the address and telephone number of the company which is supposed to have sent the repairmen there, and somebody on the premises who has called for them in the first place. The name of the company should also be displayed prominently on both their car and the boxes or bags containing tools the repairmen bring into the building. The normal amount of traffic in the building at the proposed hour of entry must also be determined carefully. The behavior and patrol pattern, if any, of the watchman or the security guards must be noted in particular and compensated for in the final entry plan.

The reconnaissance phase is followed by the planning phase. First of all, it must be decided whether the entry is to be covert or overt.

A covert entry is generally preferred, as a successful covert entry will guarantee that the enemy does not realize his secrets have been exposed. The disadvantage, however, is that a covert entry is difficult—sometimes impossible—to execute, and there is a much greater chance of failure.

A covert entry can also be used by police to acquire information without having the proper authority to enter the target building.

An overt entry, on the other hand, is much easier to perform. The disadvantage is, of course, that the enemy will be

alerted to the fact that an entry has occurred. Therefore, in order to minimize the chance of his finding out who executed the entry, as well as to maximize his concern that vital secrets have in fact been lost, the entry is frequently camouflaged as a simple burglary, executed for profit.

In either case, the planning phase consists of more or less the same type of work. However, it must be realized that the planning described in this chapter might take several weeks. An entry operation is consequently not to be undertaken on the spur of the moment.

First of all, if the target is located in an apartment complex, it is necessary to decide how to enter the building that contains the target office or apartment. This is frequently done by renting another apartment in the same building. Sometimes it is instead possible to enlist the help of the owner or superintendent, or some other worker or resident in the building. The superintendent is the preferable choice, however, as he frequently has a master key to all apartments in his building. In either case, the personal characteristics and loyalty of the helper must be researched thoroughly, so as to preclude a security leak at a later stage. If the man turns out not to be trustworthy, or none of these alternatives are viable, the team must find a plan to both enter the building and then to perform the actual break-in.

If the target is a villa, small house, or mansion, the procedure is more or less the same. A neighbor might be available, or the entry team must get into the neighborhood and perform the actual entry at the same time.

If it is impossible to secure a master key, it might still be possible to obtain and make a copy of the relevant key prior to the operation. One way of doing this is to search the owner of the key's pockets at a time when he is unable to notice the search. Such opportunities are not easy to come by but might arise in public baths or gyms. A key is not just useful when entering the premises; it is also invaluable if the operatives have to make a quick escape.

As was noted above, a sufficient number of escape routes must be prepared. If a master key or the actual key to the target area can be secured, a sufficient number of copies

should be made to ensure that no member of the entry team will be trapped in the building in case of an emergency. This might be a vital precaution.

The members of the security ring must also be experienced enough to delay any employee or resident of the target apartment who might want to enter the premises when the entry team is working. Such a delay can be caused by a member of the security ring pretending to be drunk and accosting the employee until the entry team has managed to withdraw. Another possibility is pretending to be involved in maintenance of the elevator. Minor car accidents or similar situations might also be used to effect a delay. Initiative is very much in demand here, as nobody can plan for every possible situation.

An inner security ring is sometimes also organized specifically to deal with such situations. It is not always necessary to leave the building, even if the security ring gives warning, however. Sometimes the entry team can simply retreat temporarily to a nearby office or apartment and await the moment when they can resume their work. This option is generally not available during overt entry operations, however.

Every member of the entry team should be supplied with a convincing and documented cover story explaining what he is doing on or near the premises. The contents of his pockets and his clothes must conform to the cover. If caught on the premises, he must at least manage to convince his captors that he is an ordinary burglar. The equipment brought onto the premises, as well as all bags, must also conform to the cover if at all possible.

As a final note, it is prudent to rehearse the entry several times in a safe location so that every team member knows exactly what he is to do and how he will do it. The actual entry operation should, if possible, be performed without talking or even discussing what to do, as long as the team is in hostile territory or in the target area. Remember that a chain is only as strong as its weakest link, and this also applies to an entry team. Only if every man knows exactly what he is supposed to do will the operation proceed smoothly.

OVERT ENTRY

An overt entry is performed by forced means in which the operatives completely disregard the fact that the entry will definitely be noticed. The team will simply break any locks, doors, or safes standing in the way using the easiest method at hand, without bothering with such niceties as picking locks. Alarm systems will be evaded if possible, or else disregarded. Speed and force are more important than surreptitiousness.

Alarm systems, if they merely alert a distant security company or a police station, can often be disregarded completely when using this method of entry. The reason for this is that the alerted security team or police will not proceed fast enough to reach the penetrated area in time to catch the operatives. Both police and security companies are reluctant to rush to a site when an alarm system has alerted them because the vast majority of such calls are false alarms caused by defective systems.

The overt entry team essentially acts as a team of burglars. No finesse is involved—only brute force. In some countries, ordinary criminals are actually employed by the intelligence service for this purpose, but this is not recommended, as these individuals generally are not reliable and frequently cannot keep silent about missions executed.

The overt entry team should consist of operatives equipped with crowbars, sledge hammers, and a carborundum wheel with circular saw attachment. This is an extremely hard silicon carbide grinding wheel, excellent for breaking through all sorts of hard steel and other strong materials, and thus very useful in cracking safes. Explosives might also be required, although this is less common nowadays. In the past, explosives were commonly used for safe cracking, but a carborundum wheel is much more efficient and easy to control. Batteries for high-voltage power might also be necessary if the fuses in the building blow because the power load is too high or electrical power is unavailable for some other reason.

When planning an overt entry, it should be remem-

bered that the normal means of entry—the front door, for instance—is frequently more difficult to break than some other part of the building, such as a roof or a wall. The former is often reinforced, which very seldom is the case with other parts of the building, at least in smaller houses and villas.

COVERT ENTRY

A covert entry is much more difficult to perform than an overt entry. Speed is important in this operation, too, as every minute in the area of operations brings a chance of discovery and capture. But even more important are skill and diligence. Every lock must be picked, and the means of entry must never leave any marks revealing that an entry has occurred. In fact, every part of the premises must be left in exactly the same condition as it was before the entry. As this requires considerable skill, it should not be attempted by inexperienced operatives; the chance of the enemy noticing the entry is simply too high. Furthermore, a covert entry must frequently be called off because a certain lock or safe proves impossible to pick open in the time available to the operatives.

When all the details of the planning phase are taken care of, a preliminary entry is sometimes undertaken. This entry is executed very cautiously, however, and no attempts are made to find or obtain any interesting documents in the target area. Instead, the sole purpose of the preliminary entry is to make certain that the plan is valid and sufficient expertise is available to perform the actual entry operation. At the time of actual entry, the team and its equipment are generally too conspicuous to allow for failure and the subsequent chance of exposure.

The preliminary entry must be made in absolute silence and with extreme caution. This is because voice-activated tape recorders might be hidden in the target area, and there might be any number of innocent-looking traps, such as short lengths of thread or hair, paper clips, books and papers, or other small objects positioned in a certain spot or

arranged in a special way. Such traps are set up to alert the target that somebody has tampered with his things or entered the premises. Before any object is moved, it is therefore necessary to take accurate measurements of the position of every object. This is most easily done with the help of a Polaroid camera.

There might also be more devious traps, such as a video camera and recorder initiated by a sensor capable of detecting an individual on the premises.

The operatives must also remember that many computers will register the time at which they are turned on or execute a command. It is therefore very risky to check the files of a computer, unless the operative knows exactly what he is doing. (Of course, this is never a problem with forced entry operations. As computers are valuable objects, the entire set can be taken easily, without anybody wondering why the burglars stole it.)

Yet another problem is areas covered by dust. The operative must not remove an object from such an area unless he can replace the dust in a convincing way. A small atomizer filled with talcum powder mixed with powdered charcoal can sometimes be used to simulate dust.

During the preliminary entry, the operative should also make a detailed check of the premises. He might find, for instance, that there will be a need for blackout curtains during the actual entry operation. The operative must then determine exactly how many such curtains are called for, as well as their required size and a method of attaching them to the windows. Another point to consider at this time is the number and types of safes and file cabinets. As many details as possible on them, as well as on all ordinary locks in doors and so forth, must be collected, including any numbers on the locks. It is frequently necessary for the locksmiths to know these details in advance in order to pick the locks successfully during the actual entry operation.

It is also important to find a safe place to put camera equipment and a small, portable Xerox machine during the actual operation. Preferably, this will not be inside the office or apartment to be searched, as it could preclude or

hinder a quick escape. A small, nearby cleaning storage room is ideal for this purpose. Rest rooms should be avoided, too, as they might be frequented by a person making an unexpected call to his office or apartment during the entry operation. If the chosen camera site is sufficiently remote, it might even be possible to return later to recover the equipment hidden there if a quick escape is required.

The successful execution of a covert entry requires very careful planning as well as considerable skill. In addition, it is necessary to maintain total security from interruption during the search of the target building. This necessitates the use of both an outer security ring and probably an inner security team able to delay any intruders.

A covert entry team must consist of several individuals, each an expert in his field. Among them should be a lock-picking expert, a safe expert, and one or more experts on alarm systems in order to execute the actual entry. The alarm system experts must be prepared to manipulate electronic locks and other electronic systems such as lift machinery.

Furthermore, one or more analysts capable of rapidly evaluating any found documents and at least one photographer should be present. The photographer must be equipped with several cameras, both for copying any found documents, and, equally important, snapping Polaroid photographs of the original appearance of the rooms to be searched, in order to provide a pattern for restoring everything to its original place before leaving the premises.

Nowadays, as was noted above, it is common to use a small, portable Xerox machine to duplicate any found documents. Of course, a sufficient supply of film, paper, and so on must be included in the equipment brought onto the premises. Sometimes infrared photography techniques can be used, as these require no visible light source.

There should also be an expert in opening letters, capable of opening and resealing any type of letter in a convincing way. This technique also requires a certain amount of equipment. It might even be required to bring an infrared

fluorescence detection system in order to detect traps on sealed letters or documents, or alterations to passports or other documents.

Finally, any guns or other means of dealing with individuals interrupting or noticing the entry must be decided upon. Every piece of equipment, including radio transmitters, must be tested and checked so that nothing is found missing after the team has entered the premises. Radio transmitters in particular might require a test in the target area before the actual operation is initiated. The range of radio transmitters depends very much upon the construction of the building, as different buildings disturb radio transmissions in different ways. It might also be a good idea to bring a spare camera; a broken camera in the middle of an operation is a bad excuse to pack up and go home.

During the actual entry, the premises should be entered by only one individual operative. This is to ensure that the entire group does not walk into a trap. When this operative gives the agreed upon signal, the rest of the group will follow him in.

There are several ways to prepare for a covert entry operation. One good way, already discussed above, is to secure a master key. This is sometimes possible in apartments and office complexes, as the caretaker generally needs one. The same is true of hotels. However, it is generally impossible in villas and mansions owned by private individuals.

Another obstacle might be an alarm system. Such systems, which frequently sound the alarm because of technical defects, will not be taken seriously by investigating police patrols or private security companies, however. It is therefore possible, at frequent time intervals over a period of several days or weeks, to alert the alarm system discreetly and then quickly withdraw from the area without leaving any traces. Then, during the actual covert entry, the police will be much less vigilant. This allows the entry team a longer period of time to do what they came for.

This might also be true of an ordinary guard. During the early years of the Second World War, Willis George worked

for the Office of Naval Intelligence. As was mentioned above, he planned and executed several entry operations during these years.

During one of these, he found out that a foreign consul had posted an armed guard in the private part of the consular office. Obviously, this made a covert search impossible. George therefore had to devise a means of getting rid of the guard without exposing his own operation. The guard had probably been posted there because the consulate elevator operator had become suspicious during a previous covert search in the building.

George finally decided to try to make the elevator operator appear ridiculous by causing him to behave in a seemingly overzealous manner. If the consul eventually decided that the guard was unnecessary, then he would likely dispense with such extreme measures for protecting his office.

With this in mind, George once again entered the building for the sole purpose of deliberately making some noise in order to alert the elevator operator. Then he hurriedly left the scene.

About half an hour later, the consul arrived by taxi. The elevator operator had, just as was expected, called for him. They searched the office, of course without finding any signs of an entry. The consul was angry and left after the fruitless search.

A few nights later, George repeated what he had done. Once again, upon hearing the suspicious noise the unfortunate elevator operator called the consul immediately. The consul arrived, angry and tired of being awakened every other night. Once again, their search produced no indications at all that an entry had been attempted.

The next night, as the guard was no longer posted in the office, George and his team were able to continue preparing for the actual entry.

In this context, it should also be noted that the majority of all false alarms take place in the morning between seven and nine and in the evening between five and seven. The reason for this is that these are the times when the ordinary occupants of the buildings turn the alarm systems off or on.

The police and serious security companies know about this and are therefore less vigilant during these hours.

When on the premises during an illegal entry, the operatives must think of many things. They must not, for instance, use any toilets or water faucets. This could leave traces and make noise in the plumbing pipes. Smoking is also prohibited, of course, as this leaves both traces and odor.

Finally, when leaving the premises after a concluded operation, whether successful or not, it is important to check that no piece of equipment has been left behind and that the appearance of the target building is exactly the same as before the entry. This might require polishing or even rewaxing the floor, if the operatives have entered with their shoes on. All fingerprints must be wiped clean, whether on doors, walls, or office equipment. If a safe has been opened, the dial must be reset at its original reading. If the apartment contains thick rugs on the floor, it might even be necessary to sweep them upon leaving so as not to leave any footprints.

It is necessary to realize that every situation is different from any other, so while the rules above are useful, there might be other things to think of, too. Only extreme diligence and caution can make a covert entry remain so.

Locks and Lock Picking

Lock picking can be defined as the method of opening a lock mechanism by the intrusion of special tools other than the regular key. Lock picking is not easy. It is, however, possible to open any lock without the proper key, but some locks are definitely more difficult to open than others. In this chapter, we will look at the basic types of locking devices and how they can be opened most efficiently without having access to the proper keys.

The reason lock picking is at all possible is that there are always certain tolerances built into the design of the lock. The various parts of the mechanism never fit perfectly. There will always be some diminutive empty space in which the lock-picking tools can be inserted.

An expensive lock is usually, but by no means always, designed and manufactured with less tolerances than a cheaper one. Less tolerances mean less space to insert lock-picking tools. A cheap lock is therefore almost always easier to open, as there will be tolerances large enough to insert whatever tools are required to pick the lock. No lock is absolutely pick-proof, although today there are numerous types that are extremely difficult to open. In some cases, the level of difficulty is so high that the lock is effectively impossible to pick under field conditions.

However, as the price of the lock dictates the quantity

that can be sold, the vast majority of locks are fairly cheap and consequently easier to pick open. For this reason, there is a very good chance that the lock encountered during a mission will be one of the cheaper types.

The devices used as locks today can be divided into the following general types:

- warded locks
- lever tumbler locks
- disc tumbler locks
- pin tumbler locks
- tubular cylinder locks
- magnetic locks
- combination locks

Locks of the types mentioned above appear in the following shapes:

- luggage locks
- padlocks
- vehicle locks
- mortise locks
- surface-mounted auxiliary locks

The last two categories are the two general shapes of door locks. They can be found all over the world. Although

these general types contain numerous design variations, all locks encountered will fall within one of these groups, with the exception of those that represent a melding of two different types of locking devices.

Luggage locks, pad-

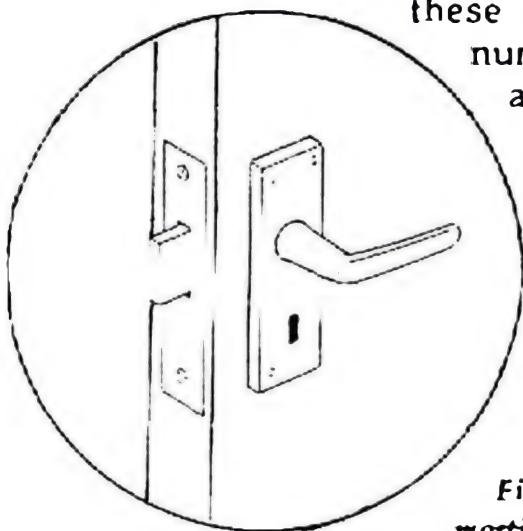


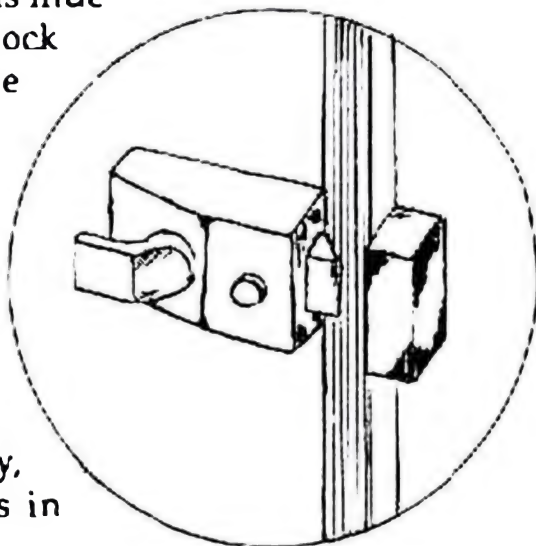
Figure 1. Rim lock (left) and mortise lock (right).

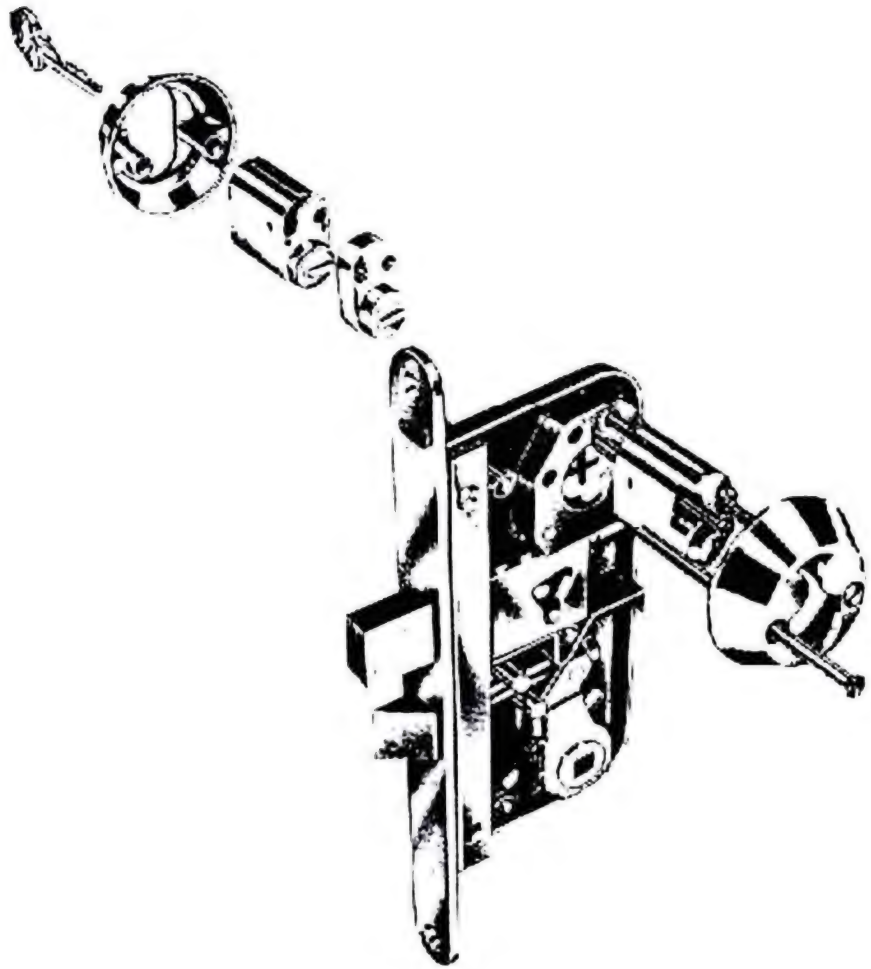
locks, and vehicle locks will be described fully later in this chapter. The door locks need to be described in more detail, however, as you are most likely to encounter these in the field.

There are basically two types of external door locks—rim locks and mortise locks (fig. 1). Rim locks are surface-mounted, screwed to the surface of a door. They usually have a spring-operated, beveled latch bolt that automatically springs back when the door is shut to hold it closed. The door is opened by turning back the latch using a key or an internal knob, or by moving a sliding handle. In most rim locks, the latch bolt is checked by a safety catch so that the door can also be shut without latching. Rim locks are also known as locking bodies.

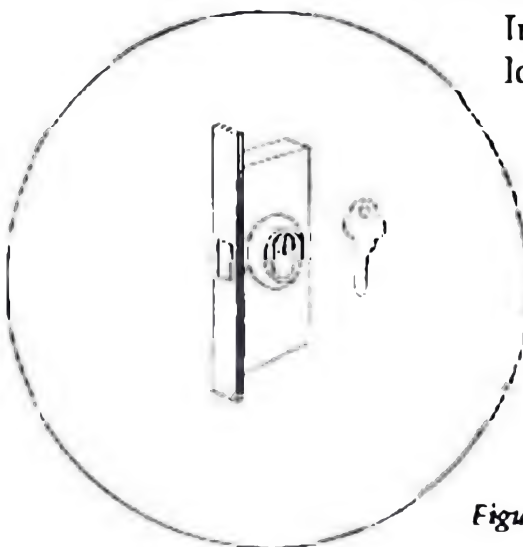
Mortise locks mount inside the door, fitting into a mortise, or slot, in the door's leading edge. They are therefore very neat and slightly stronger. However, it is generally the wood rather than the lock that gives way during a break-in, so this means little. A rim lock is therefore more commonly fitted to a thin door to prevent the door from being weakened. For the same reason, the staple of a rim lock will not weaken the door frame, as it is surface-mounted. However, the staple itself is only held by screws and can be broken away from the frame.

The simplest rim lock is the night latch. This is an auxiliary lock with a spring latch bolt that holds the door closed. The night latch functions independently of the regular lock on the door and cannot be deadlocked. The latch is operated by a key from the outside and the knob from the inside. In this lock, the spring bolt can be pushed back with a piece of flexible plastic. (For instance, see the section on transom entry, doors, and door chains in





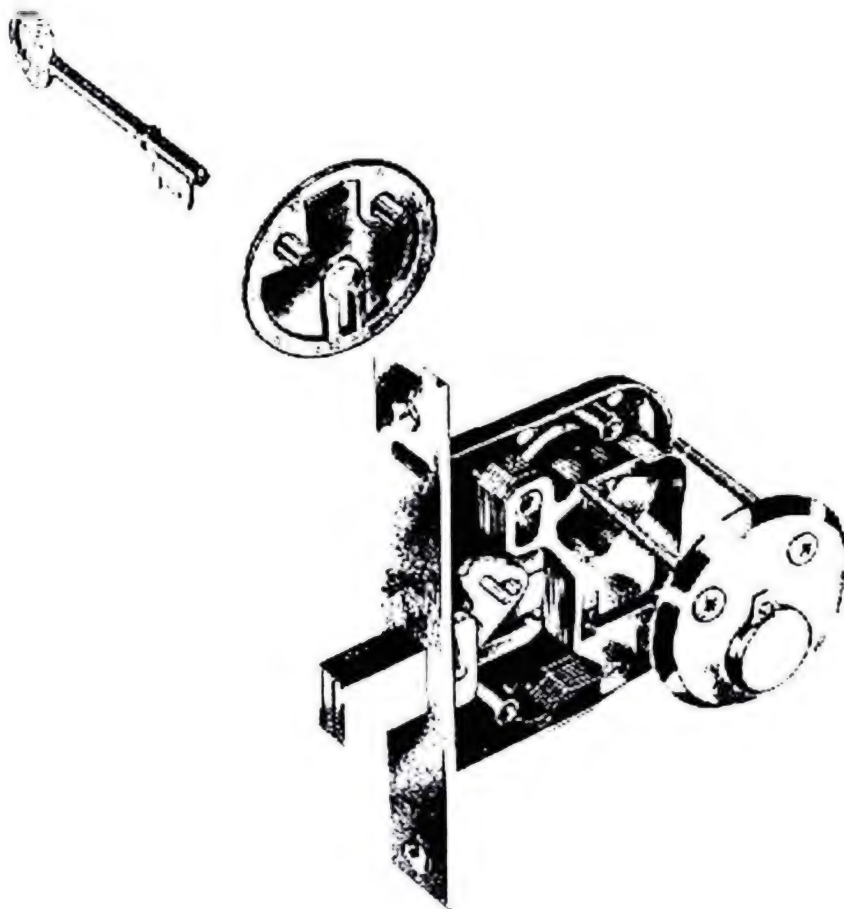
Chapter 4.) Another method is to break a small adjacent window in order to reach through and open the lock from the inside.



In practice, most simple rim locks nowadays have a deadlocking mechanism, operated by a small thumb piece from the inside, which prevents the spring bolt from being forced back.

There are also other types of surface-mounted

Figure 2. Cylinder lock.



auxiliary locks. They include dead latches (locks that can be automatically or manually locked against end pressure when projected) and surface-mounted cylinder locks used separately from another lock unit. Door chains, surface bolts, and chain bolts are also usual-

ly counted as surface-mounted auxiliary locks and will be described in later chapters.

More advanced rim locks, such as the ones with an automatically deadlocking latch (automatic deadlock) or a manually deadlockable latch, always have a spring

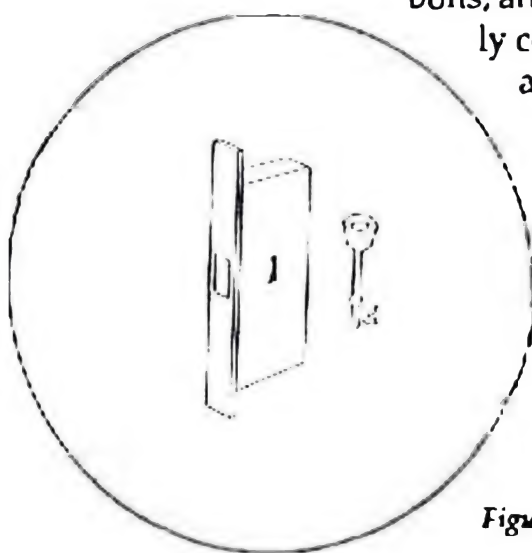


Figure 3. Lever lock.

bolt with a mechanism that prevents the bolt from being forced back when the door is shut. The internal handle can then be deadlocked by using a key, either from the inside or the outside. The lock cannot then be opened except with a key or by picking it.

Rim locks are usually operated by pin tumbler cylinders. A mortise lock, however, is either operated by a pin tumbler cylinder (fig. 2) or by flat levers in the lock case itself (fig. 3). The levers are of different heights to correspond to the cuts in the key. The number of lever tumblers determines the security level of the lock. The more levers there are, the greater the number of key variations and the more secure the lock. Five-lever locks are common, but in many countries the nine-lever lock is considered the standard today.

Some mortise locks also rely on cylinders, if the owner wants to have the same key for operating both the front and the back door, for instance. Lever-type mortise locks can also be designed to have identical keys, of course.

No part of the body of a mortise lock is visible when the door is closed, as it is concealed within the door. For this reason, the mortise lock is generally not fitted to doors less than 44 millimeters thick.

There are basically two types of mortise locks: the key-operated dead bolt and the two-bolt mortise lock, or sash bolt.

A dead bolt is a lock bolt that has no spring action. For this reason, it is always actuated by a key or a turn knob. This lock is a true deadlock. A sash bolt has both a latch bolt and a dead bolt. The latch bolt is a beveled spring bolt that is operated from either side by the door handle, while the dead bolt is operated by the key. Two-bolt mortise locks are often fitted on back and side doors, while key-operated dead bolts are fitted to front doors. The dead bolt can be operated from the inside by a thumb piece.

A deadlocked mortise lock cannot be opened from the inside without a key if it has been locked from the outside. The reason is that the bolt cannot be withdrawn into the lock case unless the key is used or the lock is picked.

WARDED LOCKS

Warded locks were first invented by the ancient Romans. The warded lock relies on one or more wards to protect the internal lock mechanism. A ward is a protruding ridge in a lock or on a key designed to permit only the correct key to be inserted in the lock. Warded locks are of a fairly simple design and can be found all over the world. They are still used in door locks in older areas of even metropolitan cities such as New York, despite the fact that they are very insecure. They are also common in old padlocks. Student locksmiths frequently use these locks for practicing lock picking.

Warded door locks are either of the rim or mortise type. Both types of locks operate on the same principle. The surface-mounted rim lock is generally even less secure than the mortise lock.

Normally there are two interior wards in the lock, positioned directly across from each other. One is on the inside of the cover, while the other is on the inside of the backing plate.

The key for a warded lock is cut to correspond to the single or multiple wards that have been designed in the lock. The key will only come in contact with the actual locking mechanism after it has passed all of the wards. Then the cuts on the key will lift the lever to the correct height and throw the dead bolt into the locked or unlocked position. As long as the dead bolt is retracted, turning the doorknob will activate the spindle and release the door.

The wards are of three possible types. One type of side ward is designed to allow only a key with a slot milled on the edge to pass (fig. 4). Another type is designed instead to allow only a key with the slot milled on the

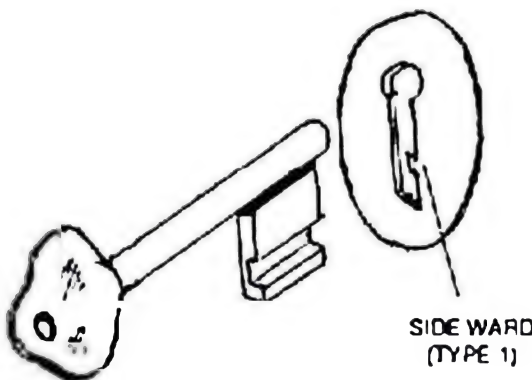


Figure 4. One type of side ward.

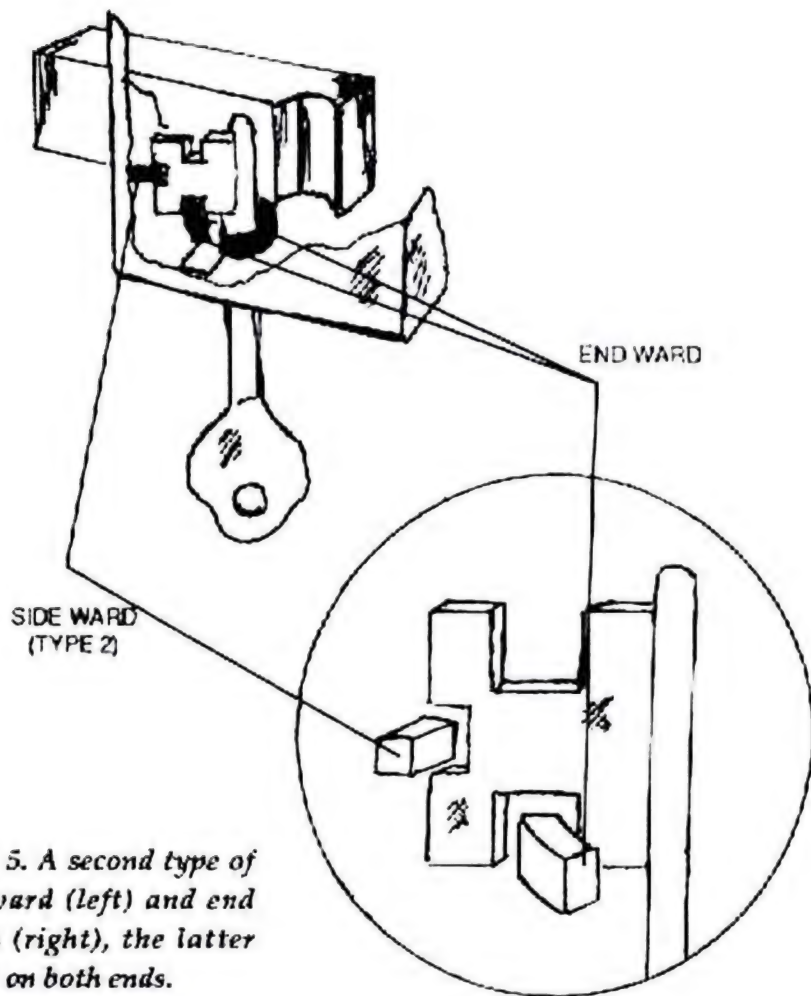


Figure 5. A second type of side ward (left) and end wards (right), the latter milled on both ends.

side of the key to pass (fig. 5). An end ward, finally, will only allow a key with a slot milled on the end to pass (fig. 5). End wards are commonly milled on both ends, as the key then can be used from both sides of the lock.

Side wards, at least, can generally be passed successfully by inserting a skeleton key—a key that has been ground down on the sides to become thin enough to bypass these wards (fig. 6). Such a skeleton key can be helpful in opening the lock, although this is by no means assured. Skeleton keys can be bought in variety stores, but generally not from reputable locksmiths. A properly made skeleton key will operate almost any warded lock whose keyway accepts it.

All the ward cuts in a skeleton key have been opened up so that only the tip that is necessary to operate the latch spring remains. Most warded locks can also be

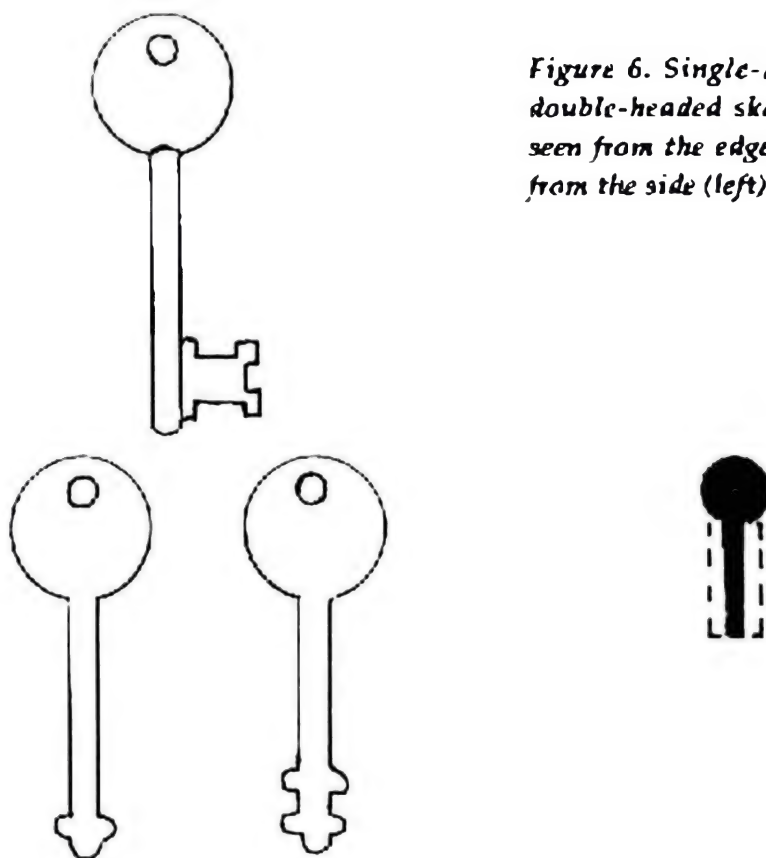


Figure 6. Single-headed and double-headed skeleton keys, seen from the edge (right) and from the side (left).

picked with a T-shaped lock pick, of course.

Nowadays many lock manufacturers try to raise the security level of their warded locks by adding another spring latch with a ward between them. Then a double-headed skeleton key can be used. The principle remains the same, but this skeleton key is designed to handle that extra complication as well.

A good locksmith with plenty of time can make a duplicate key to the lock using the technique known as impressioning. This is the method of determining the shape of the key by simply studying the lock from the outside. The locksmith will insert a key blank smoked by a candle into the lock. A key blank is a key that has not yet been cut or shaped to operate a specific lock. The smoked key blank, when extruded, will show several small marks where the candle black has been removed. These marks will tell the locksmith what cuts to make, where to make them, and how deep they must be. This is a fairly lengthy process, and

it requires some skill. Nevertheless, it is sometimes extremely useful, as the process will provide the entry team with a true copy of the key they need to use.

Because of their simplicity, warded locks are very easy to pick. Sometimes a pair of wires will be sufficient to use as lock picks. In that case, one of the wires will be used for throwing the bolt, while the other is used for adjusting the lock mechanism to the proper height for the bolt to be moved, if this is required.

The main difficulty in picking a warded lock is not to negotiate the few wards that are obstructing the pick, but to find the correct set of lock picks. Here it is important to have picks of the correct size. As was previously mentioned, skeleton keys are often easier to use. Precut blank keys are therefore often used for this purpose instead of regular lock picks.

LEVER TUMBLER LOCKS

The lever tumbler lock, or lever lock, was first introduced in the eighteenth century. These locks are still common in light security roles today. They are often found on desks, lockers, mailboxes, bank deposit boxes, and similar objects. However, now a modified, much more pick-resistant variety of the lever tumbler lock is also in worldwide use as a high-security mortise lock. In this case, the lock might use as many as nine levers or more.

It is very important to realize that although the security level of the minor lever tumbler locks is lower than, for instance, the pin tumbler locks described below, the security level of the mortised lever tumbler locks is generally significantly higher. These locks are difficult to pick.

A lever lock (fig. 7) consists of six basic parts. These are the cover boss, the cover, the trunnion, the lever tumblers (usually two, three, five, but sometimes six, twelve, or even fourteen in deposit box locks), the bolt, and the base. The lock is operated by a standard flat key. After the key has been inserted into the lock, the key is turned, which causes the key cuts to raise the lever tumblers to the correct height.

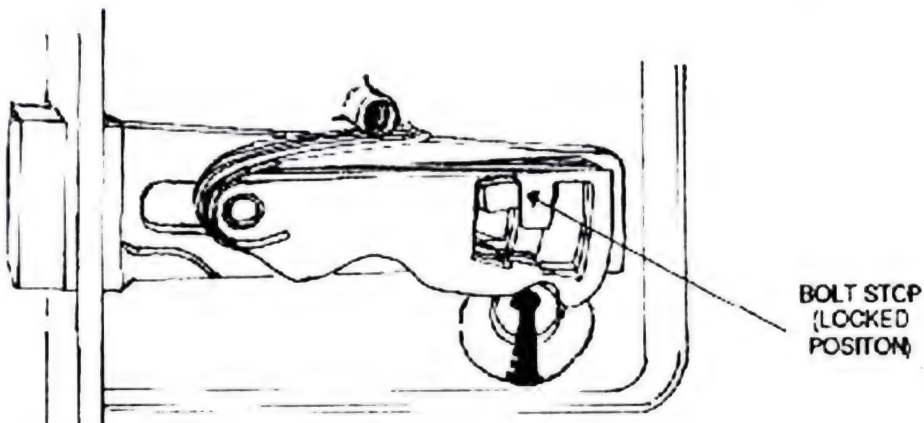
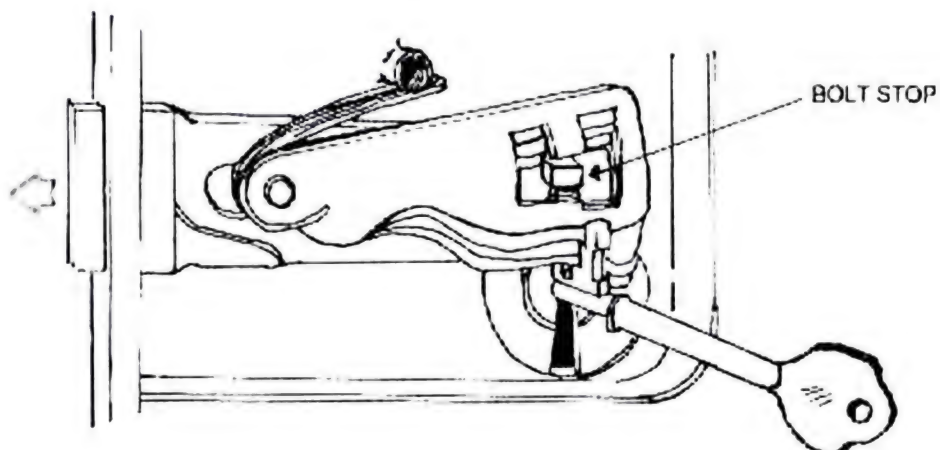
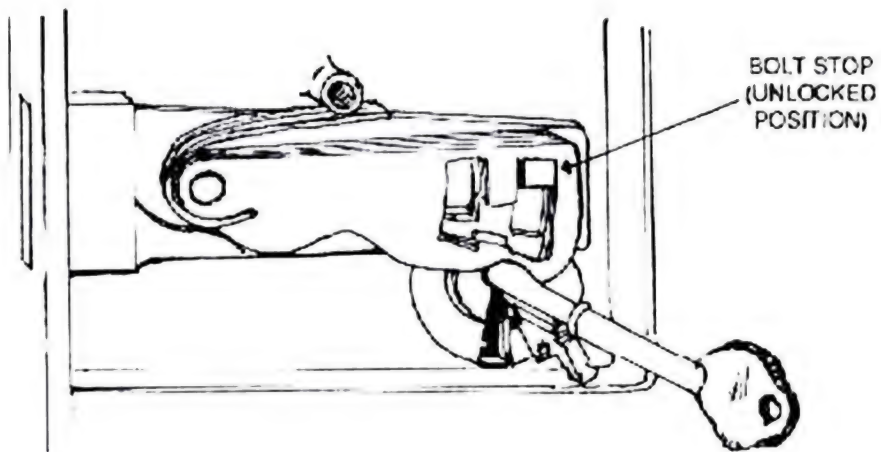


Figure 7. Lever tumbler lock.

As the levers are raised to the correct position, the gates of the lever tumblers will align and release the bolt. The bolt stop is allowed to pass through the gates from the rear to the front or vice versa; this will unlock or lock the lock.

The lever tumbler gates must be perfectly aligned, or the lock will not function. This enhances security, as the key must be cut perfectly.

The key to a lever lock is almost invariably flat. Here, too, an experienced locksmith can make a new key by impressioning. The process is much more difficult, however, than was the case with the warded lock. First of all, the locksmith must do what is generally known as "reading the lock." With a reading tool—simply a slightly bent (for a view of the tumblers), stiff length of wire, about 7 or 8 centimeters long, with a wooden handle to make it easier to hold—he can probe the narrow lock keyway. This will give him some idea of how to cut and shape the key.

The locksmith will then use the positions of the lever saddles, the part of the lever tumbler that is in direct contact with the key, as one clue to the design of the lock. The wider the saddle, the deeper the cut on the key. This process takes considerable skill and long practice. There are also locks that apparently have the same saddle width on each lever. These are even more difficult to read. Here the locksmith must attempt to determine the design by finding out how high he can raise the various levers.

In order to pick a lever tumbler lock, begin by inserting the torque (or tension) wrench. This is a special device used to apply pressure on a lock while its tumblers are being manipulated with the pick.

Push the wrench to the lowest point within the keyway, as this will give the pick maximum work space. Locate the key notch in the underside of the bolt and apply pressure (fig. 8). The bolt stop, which is affixed to the bolt, will now bring pressure on the tumblers. By exerting pressure on the lever tumblers with the torque wrench, you can manipulate them with the pick. Therefore, insert the pick into the keyway. The levers must be moved into position for the bolt stop to move through the lever tumblers' gates.

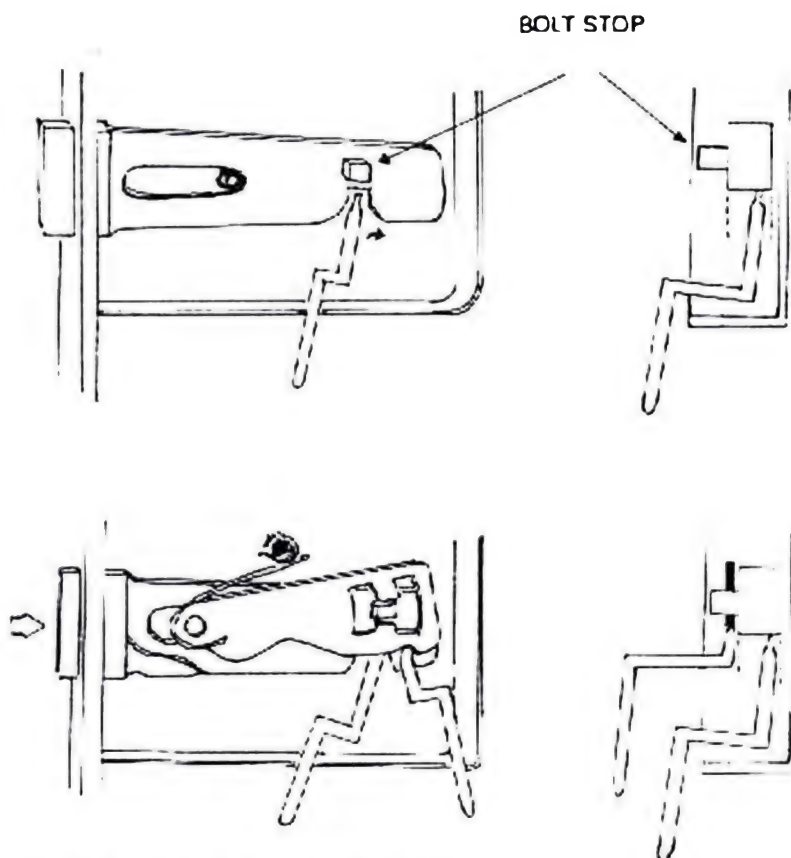


Figure 8. Picking the lever tumbler lock.

One tumbler tends to take up most of the tension, and this is the one to work on first. When this tumbler is raised to the right position for the bolt stop to pass through the gate (not too high, or it will be impossible), you will feel the tension from the bolt slacken through your wrench as the bolt attempts to force its way into the gates. This is the point at which to stop, and then repeat the process with the lever tumbler next to the raised one. When all levers have reached this point, you can get the bolt to pass through the gates by shifting the torque wrench against it. This will open the lock.

If the pressure from the torque wrench is relaxed at any time during the process, all levers in the raised position will drop back to their original positions. Therefore, always keep some pressure on. However, take care not to raise the lever tumblers too high, or they will be raised above the unlocked position. Allow the tumbler to retain its drag as it

is raised, as this will help you feel through your torque wrench when you have reached the right position.

Simpler, desk-type lever locks have two parts that must be moved in order to open them. Naturally, the lever must be raised, but the bolt must also be operated to open the lock. This can be accomplished most easily with an L-shaped lever pick. Push back the levers and catch the bolt by turning the pick until you find it. It is sometimes helpful to peer into the lock with the help of a flashlight.

DISC TUMBLER LOCKS

Lever and disc tumbler locks are related in design, although they were invented at different times. Disc tumbler locks are commonly used in garage and trailer doors, but also in many types of cabinets, desks, padlocks, older vending machines, and cars. These locks can be recognized by the fact that the first flat disc tumbler can be seen through the keyway. Disc tumbler locks are also sometimes known as wafer tumbler locks because the tumblers are shaped like wafers, or discs.

The common disc tumbler lock is generally as secure as the lever lock, but less secure than a pin tumbler lock. They are similar in appearance and in the broad principle of operation to the pin tumbler locks; however, the internal design is quite different.

The disc tumblers are flat circular or oval-shaped steel stampings that are arranged side by side in slots in a cylinder core, or plug, within the lock (fig. 9). Every disc will

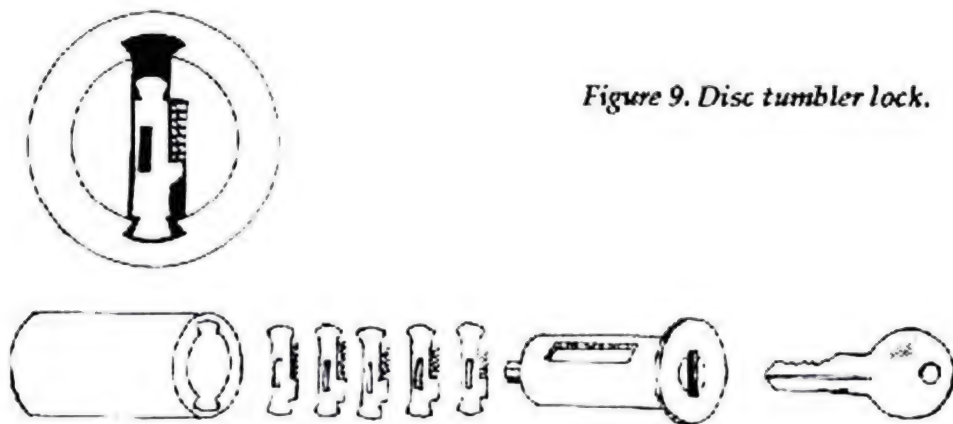


Figure 9. Disc tumbler lock.

have a rectangular cutout in the center, which matches a notch on the key bit. The disc will also have one or more side projections.

This type of lock employs a rotating core, and this is what makes the disc tumbler lock look similar to the pin tumbler lock. The core is cast so that the tumblers protrude through the core and into slots on the inner diameter of the cylinder. As long as the tumblers are in place, the core will be locked to the cylinder. The key, when inserted into the lock, will raise the tumblers high enough to clear the lower cylinder slot. They must not be raised so high as to enter the upper cylinder slot, however, as this will once again lock the plug in position. When the tumblers have been raised to the right position, the plug is free to rotate. This will operate the bolt.

The key to a disc tumbler lock looks like a cylinder pin tumbler key, but it is usually smaller. Furthermore, it will always have five cuts, while a cylinder pin tumbler key might have six or seven. Therefore, the disc tumbler lock is not very secure. As every lock has no more than five tumblers and each tumbler cutout has five possible positions, the design technically allows 3,125 different key changes. In practice, however, some variations are inappropriate, so this leaves us with only around 500 different key changes. Some disc tumbler locks used in offices, for instance in desks, are even simpler, with only 200 possible key variations.

Here, too, an experienced locksmith can make a key by impressioning. First, however, he must read the lock. In the case of disc tumbler locks, this is fairly easy. First of all, you must make a reading tool from a stiff wire. Insert the reading tool into the lock so that you can observe the discs within the lock. Raise and lower each disc by moving the tool until you can see the general positions of all of them. This is generally not difficult, as there are only five variations of the disc tumblers (fig. 10), and their position will give you a general idea of the profile to be used for the key. When this is determined, the key can be impressioned in the usual way by inserting a blackened key.

Disc tumbler locks are often used in offices. Their con-

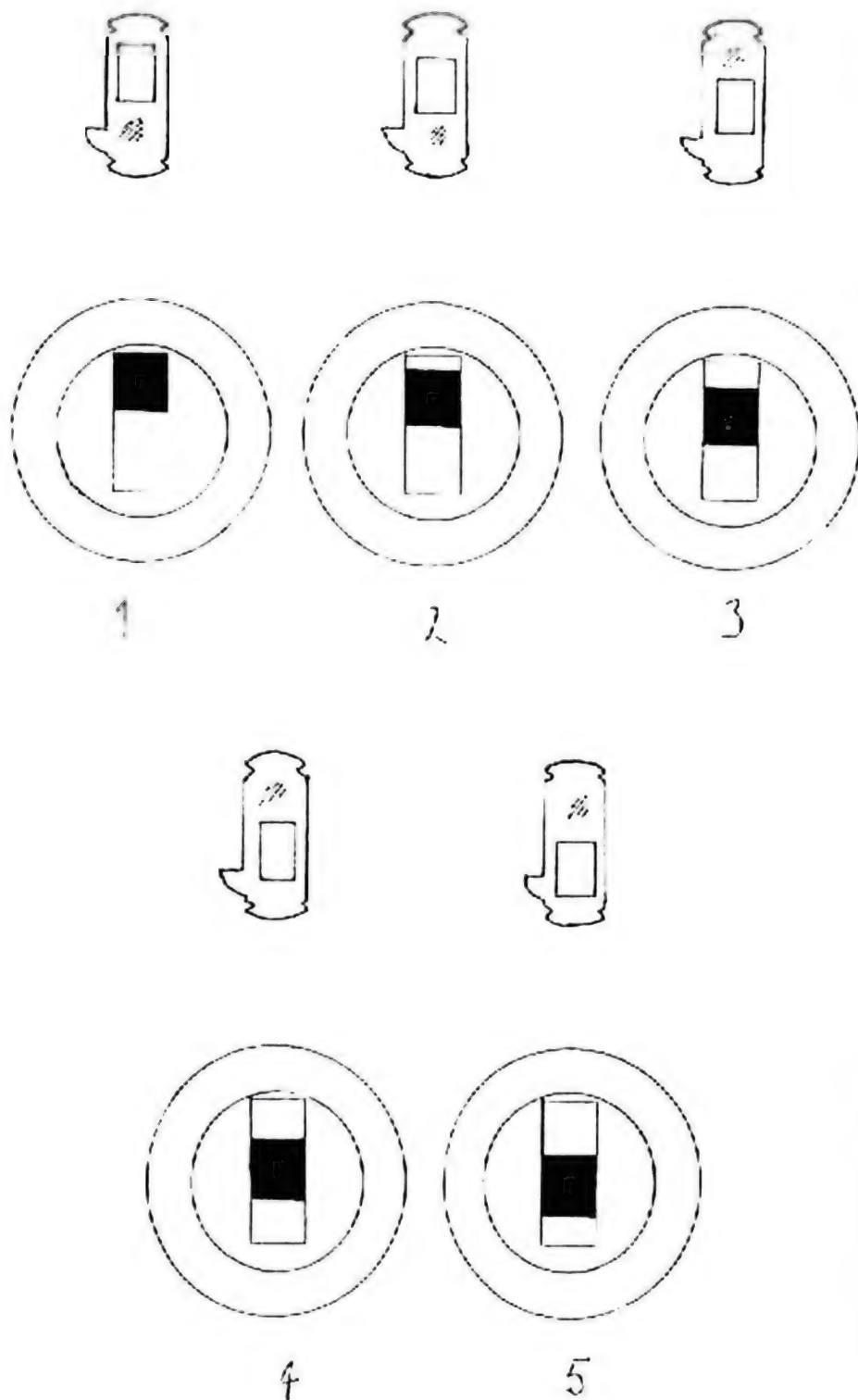


Figure 10. The five disc tumbler variations and their positions in the keyway.

struction is usually fairly simple. Sometimes a simple sliding-bolt lock will be used with the disc tumbler cylinder. In these locks, the bolt is grooved to accept a projection on the back of the plug. The projection engages the groove and converts the rotary motion of the plug into reciprocating motion, opening the lock. In some of these locks (the stronger ones), the bolt-actuating pin is cast as part of the plug (fig. 11). In this case, the plug can usually be released with a probe wire. Locks of this type are often found in drawers and cabinets.

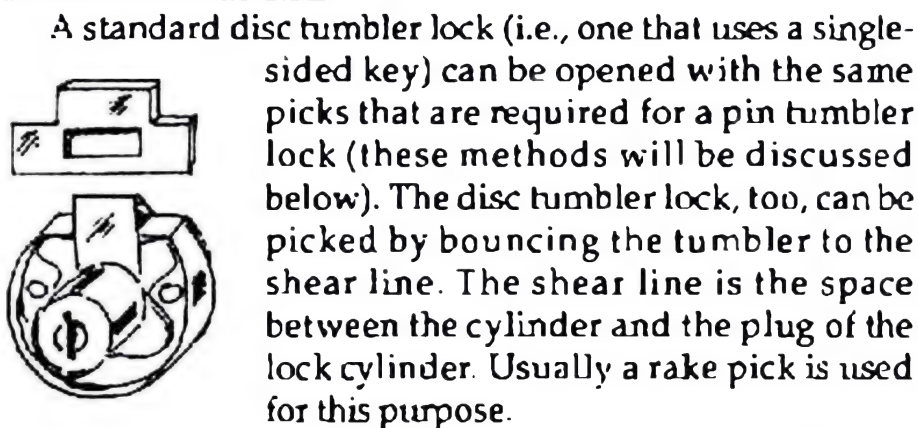


Figure 11. Simple disc tumbler lock.

A standard disc tumbler lock (i.e., one that uses a single-sided key) can be opened with the same picks that are required for a pin tumbler lock (these methods will be discussed below). The disc tumbler lock, too, can be picked by bouncing the tumbler to the shear line. The shear line is the space between the cylinder and the plug of the lock cylinder. Usually a rake pick is used for this purpose.

The bounce method is definitely the best for picking double-sided disc tumbler locks. This is a lock in which there are

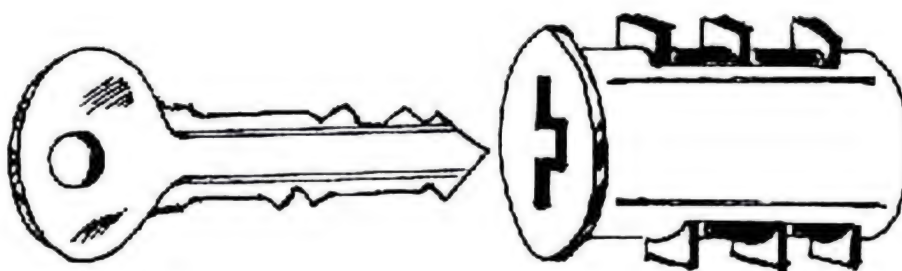


Figure 12. Double-sided disc tumbler lock.

disc tumblers protruding through the core in both sides of the cylinder (fig. 12). Such locks are also fairly common and sometimes require special lock picks. The important thing, however, is not the pick. The picking procedure is the regular one, although it has to be repeated on both sides. After the top disc tumblers have been located and moved to the

unlocked position, repeat the process with the bottom ones. Do not forget to insert the torque wrench into the keyway and apply a slight pressure to the core as the pick is pulled out.

PIN TUMBLER CYLINDER LOCKS

The pin tumbler lock was first invented in ancient Egypt. The same principle was used much later in the well-known Yale lock, introduced by Linus Yale more than a century ago. Today the pin tumbler lock is one of the most common types of locks in the world. It is used for both residential and office building locks, as well as in numerous other applications.

A pin tumbler cylinder lock is so named because it relies on pin tumblers. Pin tumblers are small sliding pins in the cylinder that work against coil springs and prevent the cylinder plug from rotating until the correct key is inserted in the keyway. Fully assembled, only the plug of the lock (the face of its rotating cylinder) can be seen. Locks of this type are generally more secure than the previously described locking devices. They can be recognized by the first pin that can be seen through the keyway. Even the shear point of the pin can sometimes be seen when looking into the keyway.

The pin tumbler cylinder is a completely self-contained mechanism that can be used with a very large number of lock sets. The basic parts of the pin tumbler cylinder are the cylinder case or shell, the plug or core (the cylindrical mechanism housing the keyway), the keyway, the upper pin chambers, the lower pin chambers, the springs, the drivers or top pins, and the bottom pins (fig. 13). All parts of the cylinder are housed by the cylinder case.

The plug is the part that rotates when the proper key is inserted into the keyway. The drilled holes across the length of the plug can vary in number, but there are usually five or six. Some plugs have as few as four or as many as seven holes. These holes are called the lower pin chambers, as they each hold a bottom pin. The upper pin cham-

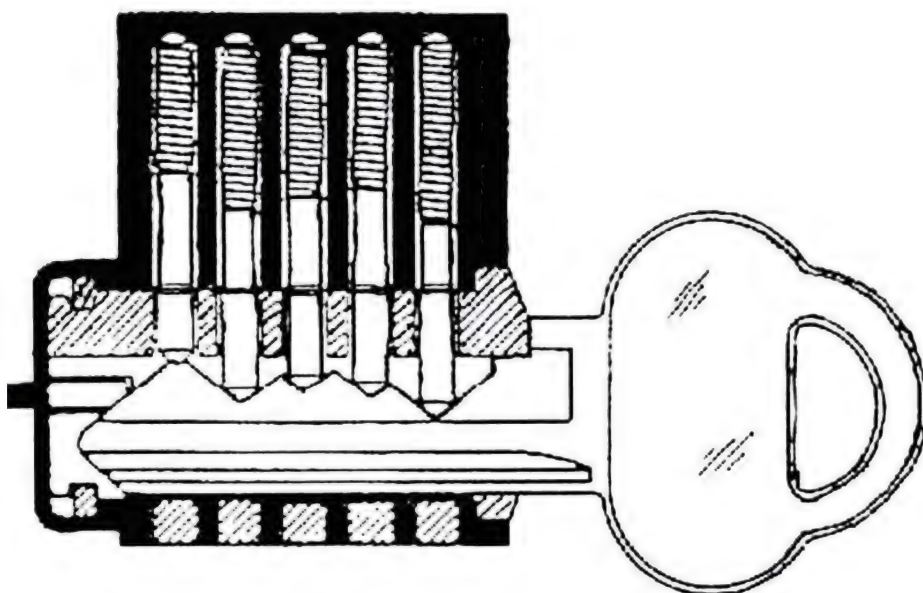


Figure 13. Pin tumbler cylinder lock.

bers are the corresponding drilled holes in the cylinder case directly above the holes in the plug. They each hold a spring and a driver.

The springs and drivers are usually of the same length. The bottom pins, however, are of different length, as they are designed to match the depth of the cuts in the key to the lock by being raised to the shear line by means of the cuts in the key.

Whenever there is no key in the keyway, the springs will press the drivers partially down into the plug so that it will not rotate. As the plug already holds the bottom pins, there is not enough room to allow more than the lower portions of the drivers into the plug.

In order for the plug to be able to rotate, there is a small amount of space between the plug and the cylinder case. This space is called the shear line. When a proper key is inserted, it will force the top of all the bottom pins and the bottom of all the drivers to meet at the shear line. Then, finally, the plug is free to rotate to the open position.

The plug is generally machined with a shoulder at its forward surface, which mates with a recess in the cylinder. If this is not the case, however, it will be possible to open

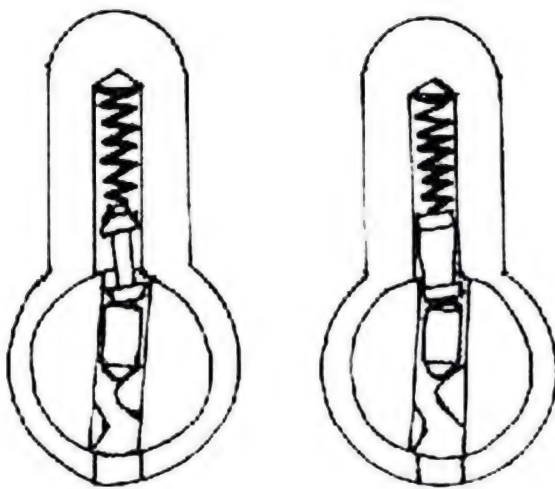


Figure 14. High-security drivers. Spool driver (left) and mushroom driver (right).

the lock by shimming the pins with a strip of spring steel. This would force the pins out of engagement and allow the door to be opened. Contemporary locks do not generally allow this, however.

The pins and the drivers will usually have a broken profile so as to make the lock more difficult to pick.

A driver with a broken profile will generally hang up before it passes the shear line. A lock with standard cylindrical drivers is consequently easier to pick. For this reason, so-called mushroom and spool drivers are fairly common in pin tumbler locks (fig. 14). Mushroom drivers are mushroom-shaped. A mushroom driver will interfere with picking the lock, as it will engage with the notched cylinder shell when you attempt to raise the pin to the shear line. The spool driver works in a similar way.

It is also possible to impression a key to a pin tumbler cylinder. The methods are different, however, than for the previously mentioned warded, lever tumbler, and disc tumbler locks. The main difference is that the key blank cannot be smoked, as the soot would wipe off when the key was inserted into a pin tumbler cylinder. The locksmith must therefore depend instead on the small marks left on the key blank itself after it has been exposed to the pin tumblers. For this reason, it is best to polish the key blank thoroughly before it is inserted the first time. The tiny scratches you are looking for will be impossible to see otherwise.

Picking a pin tumbler lock requires the ability to determine when the cylinder pins have reached the shear line. This can be felt through your tool or heard as a minute click.

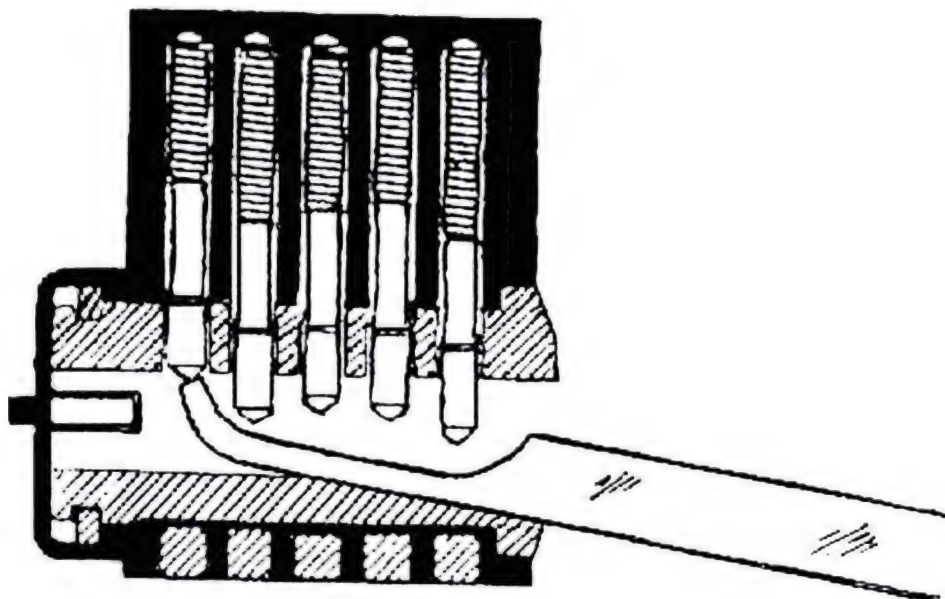


Figure 15. Raising a pin to the shear line.

A feeler pick should be used to raise the pin to the shear line (fig. 15). Be careful not to apply too much pressure, however, as the pick then will raise the pin above the shear line rather than exactly to it. If this happens, the pin will completely block the attempt to pick the lock open. Furthermore, the pin can then easily get stuck at the wrong place.

Before you attempt to raise the pins, insert a torque wrench into the keyway. The reason for this is that moving the wrench slightly to the left or right will hold the drivers tight against the plug. Then insert the pick and, when all the pins are raised to the proper position, use the wrench with just the right amount of pressure to rotate the plug to the unlocked position and open the lock. Never use too much force. Usually only a delicate but firm touch is required to rotate the plug.

It is, of course, difficult to first raise, and then keep all of the pins at the shear line. But the fact that the cylinder pin holes in most locks are not perfectly aligned helps the operative to hold one pin at the shear line with the tension from the wrench while working on the next one with the pick.

The first pin to be raised should preferably be the longest. This is usually the tumbler that takes up most of

the tension. Beginning with the longest pin also allows the locksmith to progress from the smallest amount of pick movement up to the greatest. When picking the lock, you will notice that the plug will move slightly for every pin that reaches the shear line. Remember that this movement can also be felt through the torque wrench. This makes it easier to notice when a pin has been raised successfully.

If one of the pins is raised above the shear line, you must release the tension and start again. Less tension is then required when you make the renewed attempt. It is very difficult to judge the amount of pressure necessary to raise the pins in a lock, as even two locks of the same type can react in a totally different way. An experienced locksmith will vary the amount of pressure from light to heavy, depending on what is required. This is more easily said than done, of course, but experience will help.

Mushroom drivers, when encountered, present a special problem. It is easy to describe how to pick these locks in theory, but a large amount of practice is required to do it successfully on a consistent basis. The secret lies in feeling the exact moment at which the driver is engaging the notched cylinder, but before it becomes completely stuck. At this point, slightly release the pressure on the pin before you once again attempt to raise it. With any luck, the driver will have slipped back so that you can now raise it straight up until it is above the mushroom-shaped trap. When the pin is safely raised to the unlocked position, immediately increase the tension on the wrench so that it will not slip down again. Some locksmiths use a spring-loaded wrench for this purpose.

Another way of picking a pin tumbler lock is to use a rake pick or a diamond pick (see Chapter 3) to bounce the pins to the shear line. This process consists of inserting the pick fully and then quickly withdrawing it while applying light tension on the plug. This motion often throws the pins apart because of inertia. The area at the shear line will open up, permitting the plug to rotate. This technique does not work on all types of locks, however.

A rake pick is sometimes also used to rake the lock

open. This is not recommended, as some locks will be damaged. Another point to consider is that merely forcing the pick rapidly in and out of the cylinder (raking) will only bounce the pins above the shear line. Delicacy is required, so if you do not have sufficient skill to pick the lock open, I would strongly recommend bouncing instead of raking.

A very worn cylinder, especially one with loose plugs, is frequently quite easy to open with the bounce method. Make a few attempts before you try to pick the lock. If four or five tries do not open the lock, however, it is probably better to stop wasting time bouncing it, as it will not open in this way.

It should be remembered that some types of high-security locks are much more difficult to pick or impression than ordinary ones. The Medeco locks, for instance, are very pick-resistant, as they are based on a dual-locking principle. The rotation of the plug in such a lock is blocked by the secondary locking action of a sidebar that protrudes into the cylinder case. The pins have a slot along one side, and they must be rotated so that this slot aligns with the legs of the sidebar. The tips of the bottom pins are chisel-pointed, and they are rotated by the action of the tumbler spring seating them on the corresponding angle cuts on the key. The pin tumblers must therefore be elevated to the shear line and rotated to the correct angle simultaneously, to allow the sidebar's legs to push into the pins before the plug will turn within the cylinder case. Picking such a lock successfully in the field is generally not likely, though it might conceivably go well under laboratory conditions.

Medeco cylinders and other cylinders of similar resistance are also protected from physical attacks, including wrenching and drilling, by hardened, drill-resistant steel inserts in the lock. Two hardened, crescent-shaped plates within the cylinder case protect the shear line

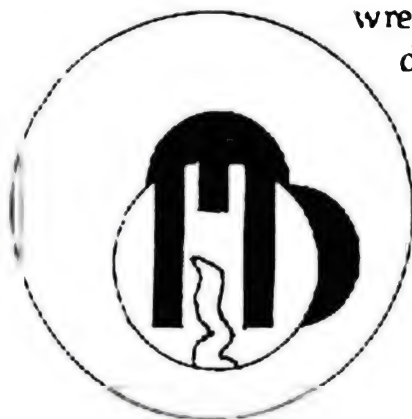


Figure 16. Protective inserts on the face of high-security cylinders.

and the sidebar, while hardened rods within the face of the plug and a ball bearing in front of the sidebar protect these areas (fig. 16). These inserts are fairly good for protecting the lock cylinder against drilling, but of course the door, other parts of the lock set, or even the wall, might still be easy to breach by physical attack.

High-security locks are generally more resistant to impressioning than ordinary locks as well. Another feature of many high-security locks is that the factory usually maintains control of the key system. The owner must present an I.D. card and sign a special order form to obtain extra keys. These keys, often known as "registered" keys, cannot be manufactured without special equipment, usually available only in a price range prohibitive to ordinary locksmiths. The key can therefore only be copied by the lock manufacturer or its authorized affiliates.

TUBULAR CYLINDER LOCKS

The tubular cylinder lock is a variation of the standard pin tumbler cylinder lock. As the latter locks became extremely popular, that popularity very quickly extended to the tubular cylinder lock as well. Today these locks are generally relied upon as high-security locks, and as they are very dependable for their price range, they can be found anywhere in many roles, such as key-in-knob locks and desk locks. Yet other common variations are the cylinder locks used on coin boxes, many coin-operated washing machines, and numerous modern vending machines. Larger versions are used as protection on automatic teller machines and in some banks.

One other important application for the tubular cylinder locks is alarm systems. They might be used to protect the control unit or act as a key switch to the entire system. The tubular cylinder lock is a real pin tumbler lock that basically works like any ordinary pin tumbler cylinder lock. The lock and its key are tubular, however, and the pin tumblers are arranged in a circle (fig. 17). In this arrangement, all of the pins can be seen from the outside.

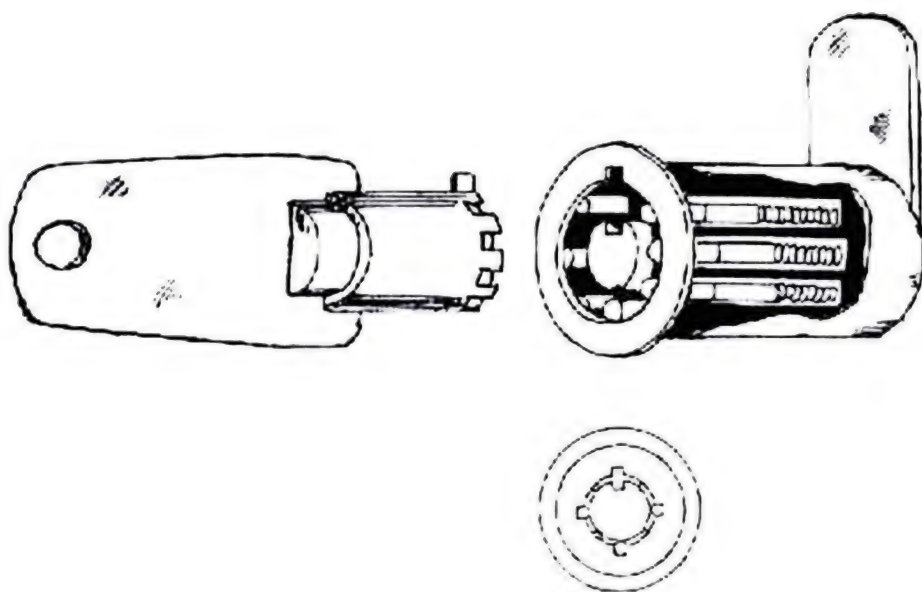


Figure 17. Tubular cylinder lock.

As is the case with the standard pin tumbler lock, the plug will rotate to operate the cam when all the seven or eight pins in the plug have been positioned at the shear line. A tubular key has a hollow, cylindrical-shaped blade that has indentations around its rim. There are usually seven or eight indentations, corresponding to the number of pins in the lock. Exactly as in an ordinary pin tumbler lock, the pin tumblers will be pressed in position by the cut of the key.

A tubular cylinder lock can be picked with a straight pin and a thin but square-shaped torque wrench (fig. 18). It is not easy, however, as you will generally have to pick it several times in order to accomplish the unlocking radius of 120 to 180 degrees. Another problem is that the cylinder will lock after it has been turned slightly. Furthermore, if the lock is left only partially picked, the key will not be able to open it unless you pick it back to the locked position. This will usually take a considerable amount of time. Another option is to use a special tubular lock-picking tool, such as is used by regular locksmiths (fig. 19). Many locksmiths will not bother with this, however, and instead simply drill out the lock if the key is lost.

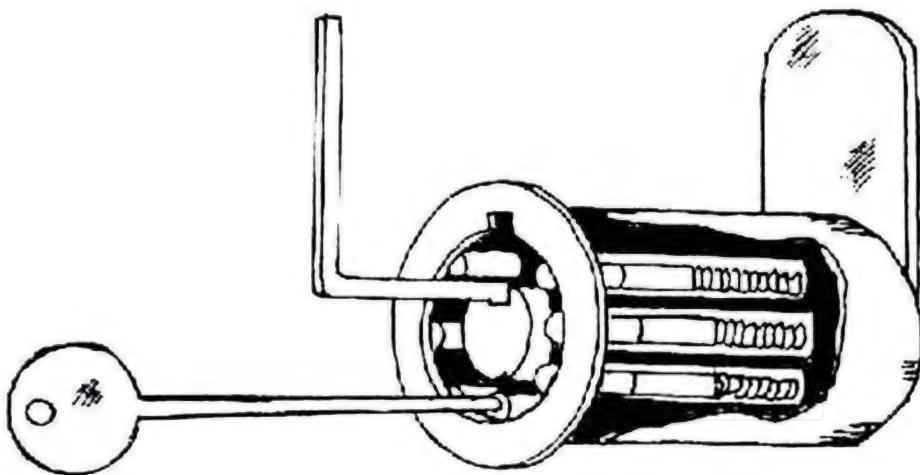


Figure 18. Picking the tubular cylinder lock.

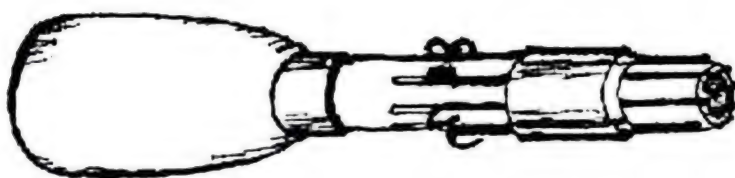


Figure 19. Tubular lock-picking tool.

The tubular lock-picking tool is a hybrid that picks and acts as a torque wrench at the same time. Actually, it does not pick as much as it impressions the lock. The tool has seven or eight (depending on the type of lock) steel fingers that adjust themselves to correspond to the cut depth of the original key. These fingers are held in place by a rubber sleeve or a strong rubber band. The rubber band will be tightened, or another rubber band will be added, once the lock opens, so that the steel fingers will remain in the correct position. At this point, the tool can either be used as a key to open the lock or as a pattern to cut a permanent, regular key.

VEHICLE LOCKS

Vehicle locks can be of almost any type, including the previously described disc tumbler and pin tumbler locks. However, it is also quite common that a vehicle lock instead relies on the sidebar principle. The sidebar lock is a more

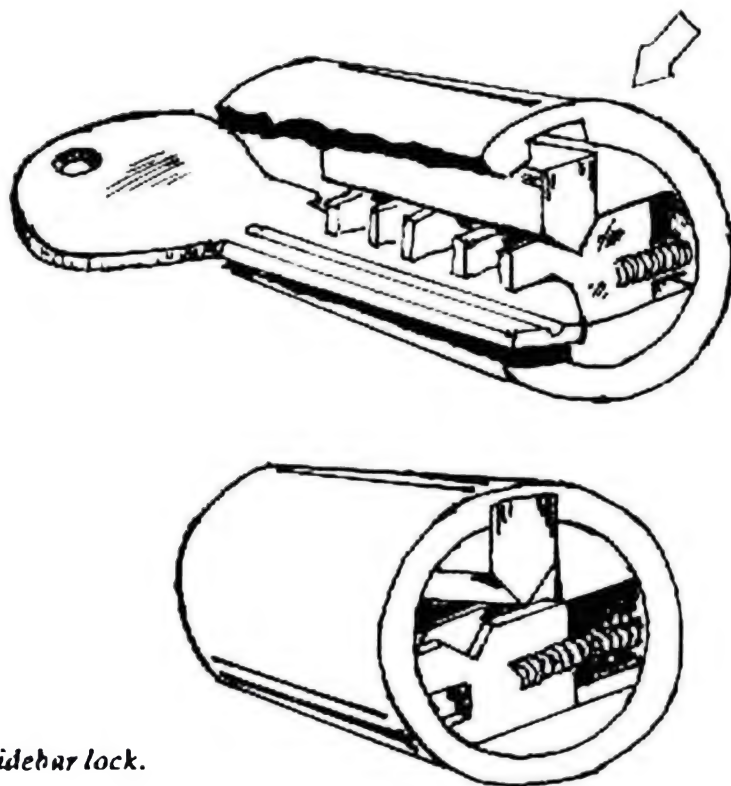


Figure 20. Sidebar lock.

specialized vehicle lock. In fact, it is a variety of the disc tumbler lock. Sidebar locks are commonly used for ignition, door, and trunk locks. They are fairly simple in construction (fig. 20). There are disc tumblers inside the lock with V-shaped notches in their sides. When the right key is inserted and engages the tumblers, the key aligns them so that the spring-loaded sidebar moves out of the cylinder and into the plug. The plug is free to rotate when the sidebar has passed the shear line, which will unlock the lock.

Although the construction of the sidebar lock is simple, the sidebar makes the lock difficult and time-consuming to pick. There is no way to determine when the sidebar will fall in place, as it is impossible to hear or feel the tumblers align with the shear line. Here experience is necessary, unless you want to drill the lock open. Then an L-shaped wire can be used to put pressure on the sidebar while you rake the disc tumblers into place. Such a method will, of course, leave very clear marks, proving that the lock has been tampered with.

The sidebar principle is also used on certain pin tumbler cylinders. Sidebars will only be found in high-security locks, described in Chapter 1.

MAGNETIC LOCKS

Magnetic locks work on the principle that identical magnetic polarities repel each other. In a magnetic lock, there will be a number of small magnets arranged in a certain order. The key contains the same number of magnets. However, these magnets are arranged so as to repel the magnets in the lock. The polarities will therefore be arranged in the same way both on the key and inside the lock. When the magnets inside the lock are repelled, a spring-loaded bolt will be moved to open the lock (fig. 21).

It is impossible to pick a magnetic lock. In an emergency, however, the lock can be breached by exposing it to a suffi-

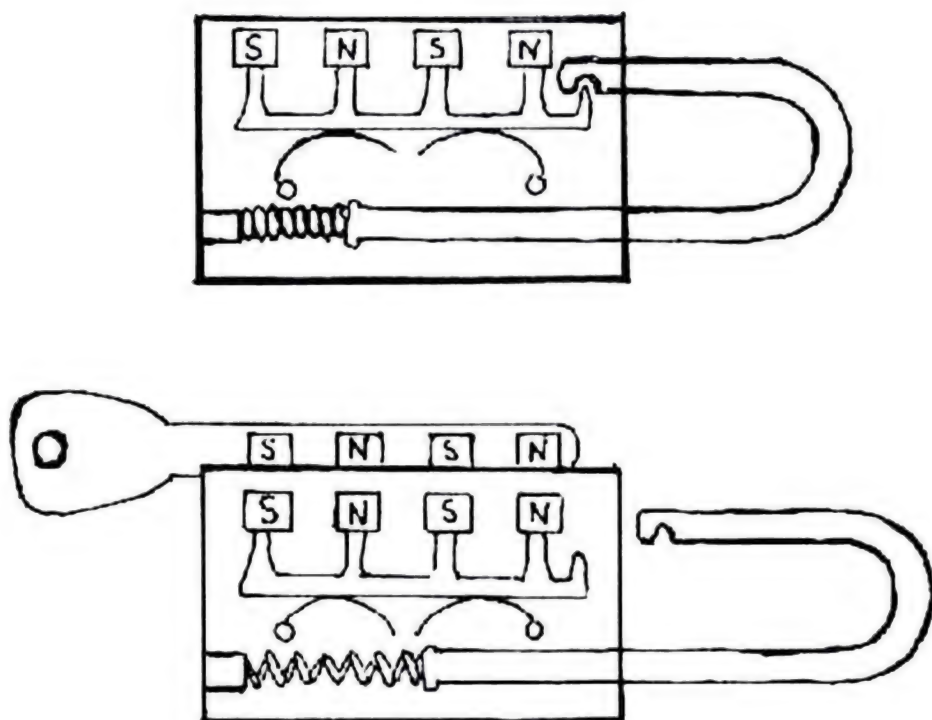


Figure 21. Magnetic padlock.

ciently strong, pulsating electromagnetic field. If the shackle (most magnetic locks seem to be padlocks) or the bolt is pulled repeatedly, the lock will then spring open. However, the electromagnetic field is likely to change the magnetic properties of the magnets in the lock permanently. If this happens, the real key cannot open the lock at a later time. The intrusion will thus be detected easily. The electronic field can be created by a portable field instrument. Of course, a sufficient power source is required.

It should be noted that magnetic door locks are also used sometimes. They are normally opened by a metal or, more commonly, plastic card containing a magnetic strip that has been coded with a certain magnetic combination. The internal mechanism is the same, however.

SIMPLE SUITCASE LOCKS

Almost all suitcase locks are of the simple, warded type. They have only a primitive bolt mechanism to keep the case closed. A very few suitcase locks rely instead on a lever-type mechanism. The lever suitcase locks are usually recognized because of the fact that the key will go half a centimeter or deeper into the lock before turning. A warded lock will be much shallower.

It is easy to make a skeleton key that will open most types of warded suitcase locks. Almost any suitcase key can be used for this purpose. Alternatively, simple suitcase locks can be picked with a special lock pick (fig. 22), easily manufactured from a strip of steel. The lock pick is merely inserted into the keyway, and when the bolt is located, the pick is turned to manipulate the bolt. This will open the suitcase.

SAFES AND COMBINATION LOCKS

A combination lock is one that may or may not be operated with a key but can always be operated by entering a combination of numbers or other symbols. This is done either by rotating a dial or pushing buttons.

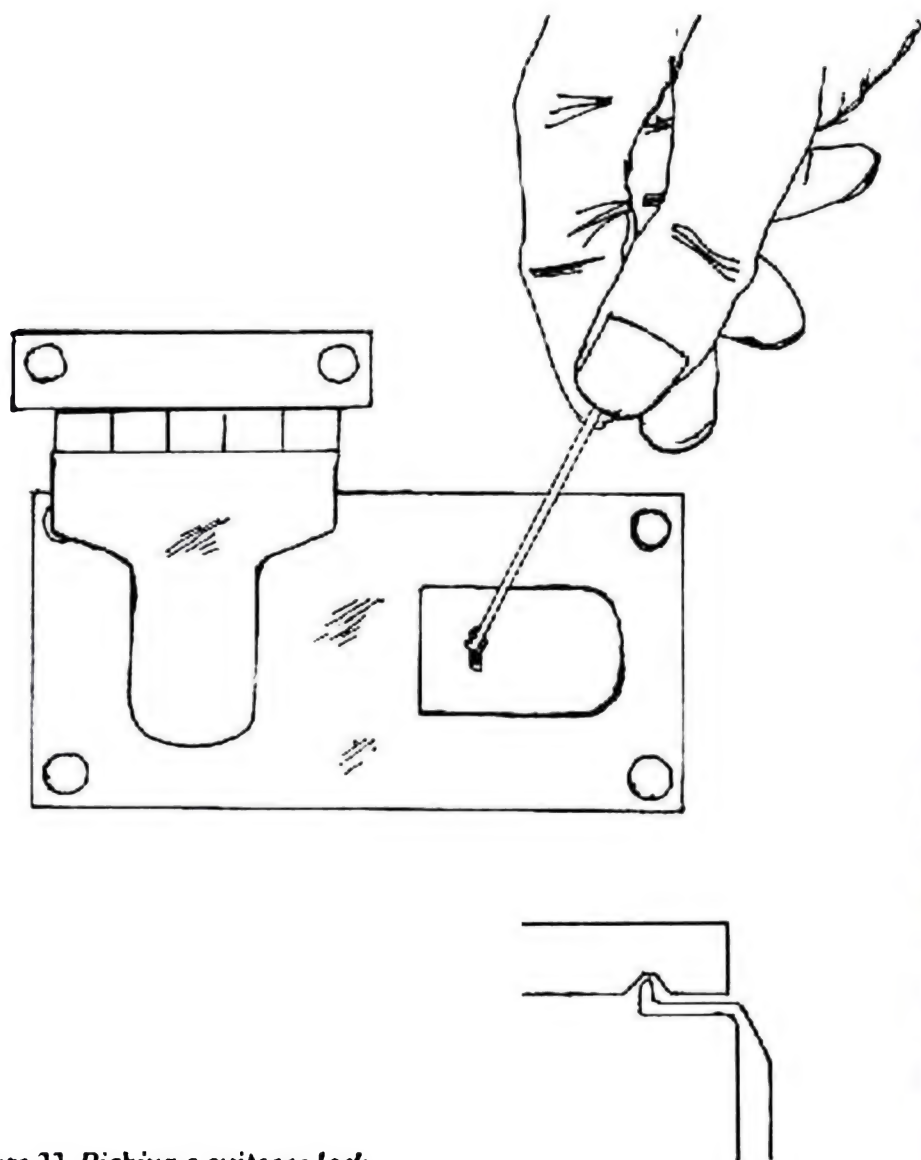


Figure 22. Picking a suitcase lock.

The most well-known combination lock is the safe combination lock. Such a lock consists of a series of interconnecting wheels that rotate around a central core. The device is controlled in its revolutions by an outside combination dial.

All combination locks of the safe type operate on the same principle, even though there are internal differences between different types of locks. An internal wheel pack will be rotated by manually rotating the external combination dial. The wheel pack consists of a series—usually three but

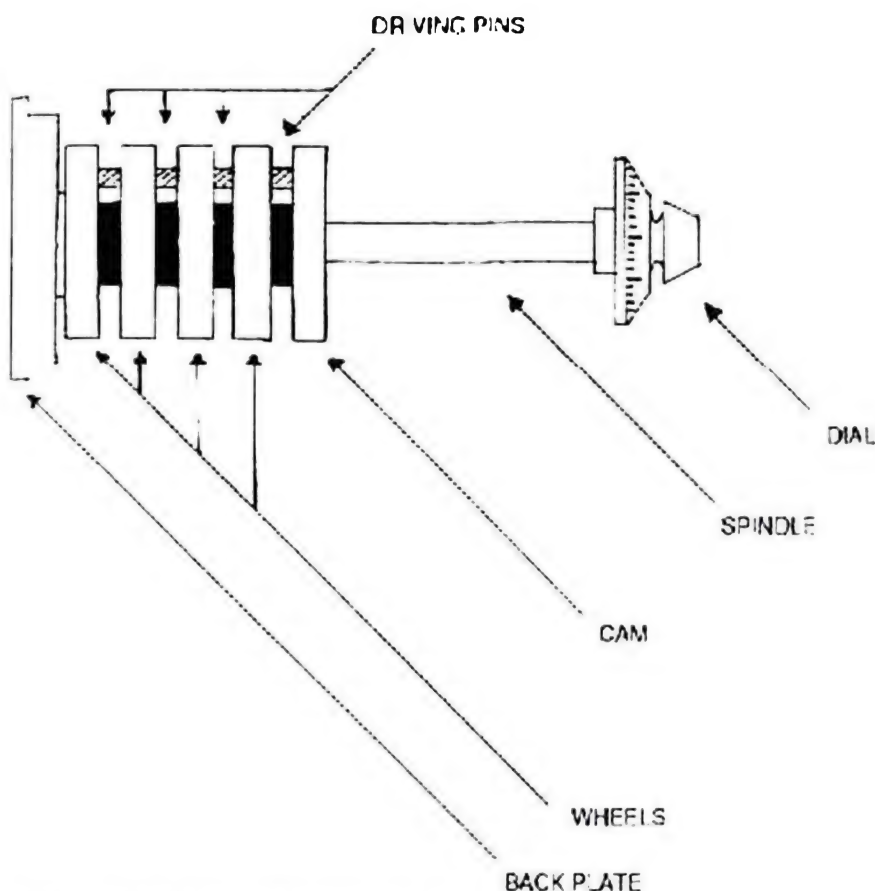


Figure 23. Dial combination lock.

sometimes four—of interconnecting wheels, or tumblers. As the dial has one hundred different numbers, or positions, a three-wheel mechanism will have almost a million possible combinations. The four-wheel combination locks have almost 100 million possible combinations. Each wheel is designed to align its gate with the bolt-release mechanism only after a certain number of revolutions and a certain degree of rotation. This design can be programmed quite easily so that the combination that will open the lock can be changed according to the owner's wishes.

Basically, a combination lock of this type works in the following way. In addition to the wheels, the complete mechanism also consists of a dial, a spindle, and a driving cam (fig. 23). These devices form the driving mechanism that moves the wheels into locked or unlocked position.

The wheels are moved by driving pins that are affixed to the back of the driving cam as well as to the wheels. These driving pins will engage and disengage the wheels as the cam revolves according to the movement of the dial. When the dial (by way of the cam) has set all wheels in the right position and is revolved slowly either back in the opposite direction to the last combination number or, in newer safes, revolved back and then forward once again, it will operate the bolt of the lock to the open, unlocked position.

The wheels are always rotated in order, and the number of turns depend on the number of wheels. The most common lock type, the one with three wheels, requires a 3-2-1 rotation sequence, while most high-security combination locks have four wheels and require a 4-3-2-1 sequence. The combination dial is always rotated (in the basic model) first three turns, then two turns in the reverse direction, and finally, in the opposite direction again one turn. Most four-wheel combination dials are designed to begin rotating to the left, but this is not universally true. Likewise, most three-wheel combination locks are designed to begin rotating to the right. There are, of course, differences between different types of safes. As the wheels are rotated, the gates will be aligned by stops, one for each wheel and one on the wheel-pack mounting plate. The bolt will be free to release only when all gates are aligned.

Older and inferior types of combination locks can be distinguished by audible clicks when the wheels rotate. This allows a skilled individual to manipulate the lock without knowing the combination in advance. Contemporary combination locks have at least three false gates in every wheel (fig. 24), so that manipulation will be much more difficult. It can still be done, but only by an expert who has had lots of practice as well as special training and knows the peculiarities of the particular type of lock he is working on.

Manipulating a combination lock in this way is a matter of touch as well as hearing. The latter is usually assisted by using an electronic stethoscope, but the sense of touch can only be developed by long training. The process can be de-

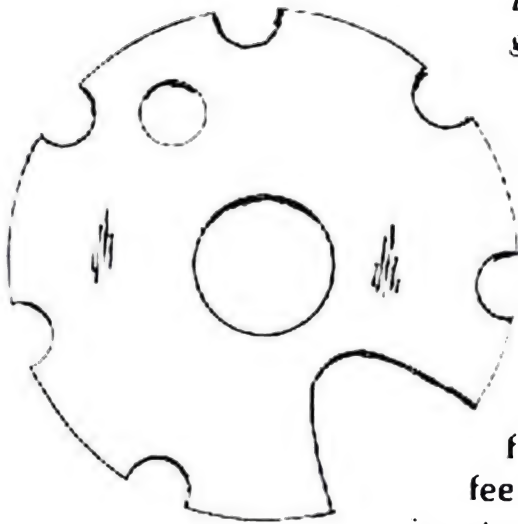


Figure 24. Wheel with six false gates.

scribed in the following way, although the inexperienced should not attempt it during a real operation.

Rotate the combination dial slowly until you hear a very faint click. You will then feel that the bolt is hesitating, touching the *far side* of the gate. At this point, move back one number on the dial and note this number. This is the first number of the combination (unless it happens to be a false gate, of course). Then turn the dial in the reverse direction and proceed slowly until you have passed the first number two or three times, depending on the type of lock you are working on. As you continue to turn the dial, you will notice that the bolt touches the far side of another gate. Once again, note the number preceding the one at which this occurs. This is the second number of the combination. Then turn the dial in the reverse direction—the original direction—once again until the process repeats itself.

After following this procedure, if you have not been tricked by any false gates, you will have the correct numbers of the combination. However, it is by no means certain that you will have them in the right order. This is no great problem, though, as you can determine the right sequence simply by varying the sequence of the numbers until you hit the right combination and the lock opens.

The existence of several false gates will naturally delay this process considerably, but the working principle remains the same. Remember, though, that practice and more practice is the only key to success. No type of lock picking can be learned properly in a short time, and this is especially true for combination lock manipulation.

Another important thing to remember is that there will always be at least a certain number of divisions on the dial between the different numbers of a genuine combination. This is to avoid any possible malfunctioning within the combination lock mechanism. This means that if you have determined two numbers that are too close to each other, or to zero, then one of them will almost certainly be false.

One important point that will assist the manipulator should be mentioned here. It is very common that the owner of the safe does not realize that the dial must be revolved completely a number of times (four times for a three-wheel lock and five times for a four-wheel lock) in order to lock the safe properly. If the dial is only partially rotated, the lock will not be locked properly, as only the last wheel will have been disengaged from the unlocked position. The remaining wheels will, of course, remain in the unlocked position. Naturally, this will greatly benefit the intruder who tries to manipulate the lock open.

Of course, the intruder will not know if it is locked properly or not. He will also be unaware of whether the dial, if the lock was improperly locked, was last turned to the left or to the right. To find out these important details, he must first of all turn the dial very slowly in either direction, simply to feel whether the driving cam is engaging the wheel or not. If it is, he must reverse the direction of the dial at once without going further, or he will lock the lock. If he can turn the dial in the opposite direction without the driving cam engaging the wheel, the lock is not locked correctly.

When it is in this way determined that the lock is improperly locked, the operative will move the dial to the position which he knows from previous study is the one in which the gate of the cam will be aligned opposite to the fence. This is generally position five or ninety-five, but it varies in different types of safes. By depressing the dial, and possibly moving it slightly to the left or right, he now attempts to cause the wheel to align itself in order to open the lock. If the wheel is only slightly disengaged from the unlocked position, and if the operative is lucky, this simple procedure might open the lock.

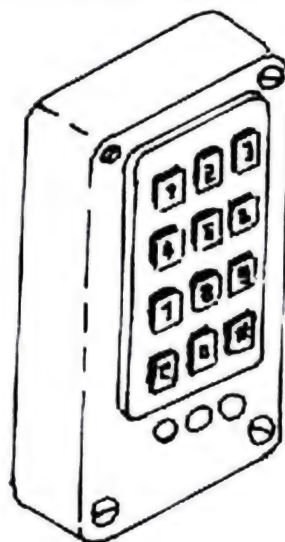
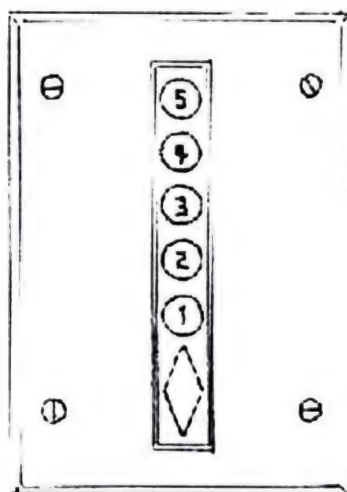
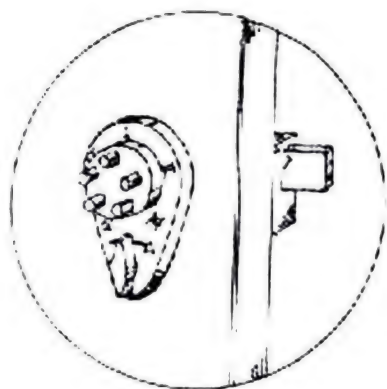


Figure 25. Push-button combination locks (top) and a digital keypad lock (at right).

Unfortunately, it is much more common that the last wheel of an improperly locked combination lock is completely disengaged. Then the intruder must concentrate instead on finding the correct number on the dial that will bring this wheel to the unlocked position. This can be done in the regular way described above. Only one number need then be found in order to unlock the safe.

Yet another point to consider is that somebody who is too careless to lock his expensive safe properly will probably use an easily remembered combination. Certain numbers, such as his birthday, might have some meaning for

him, or he might have used numbers divisible by five or ten. Combination lock manufacturers advise against such combinations, but because easy combinations are easy to remember, careless individuals still use them. It might also be worthwhile to search the room for a written note of the combination. Often such a note can be found in a desk drawer or in a notebook on a nearby table.

Some combination locks are interlocked with timer locks. This will effectively keep the lock closed until a certain time. Such advanced locks are generally only found in bank vaults, however, so they rarely present a problem.

Nowadays push-button combination locks (fig. 25) and digital keypad locks are also in widespread use. The digital lock is an electronic lock that can only be opened by keying in the appropriate number code. The push-button combination locks usually consist seemingly of only a control knob and a number of push buttons to control the lock. They are sometimes electronic, but not always. Mechanical versions are also common. Nevertheless, these locks are classed as combination locks, as they have no key. Push-button combination locks are now becoming more and more common in hotels, motels, and government institutions, for instance. Many companies also use them.

In companies and institutions, some high-risk areas can be protected by two locks, an ordinary one locked after office hours only and a keyless push-button lock allowing access by the staff during the daytime. Hotels and motels frequently find that combination locks of these types save time and money, so they are becoming more popular each day. The combination can be changed every time a guest has checked out. Therefore, the level of security is high.

Digital keypads are often used at the common entrance to an apartment or office building. Unlike some push-button types, these locks are always electronic. The lock will be opened when somebody punches the correct number code.

The standard push-button combination lock has five push buttons. The combination, pressed in the right order, will allow the knob to be moved and the lock opened from the outside. This lock can be opened with the combination only.

Another model is the key bypass lock. This lock can be opened with either the combination or the key. Employees or tenants use the combination, while senior management personnel will use master keys. This lock can be picked. A lock of this type has no special advantages, so they might be less common in the future.

Most, but not all, of these locks will include an automatic spring latch that locks the door when it is closed. This is to ensure that nobody forgets to lock the door again after entering. Another common feature is a face plate shield to prevent anyone from observing the push button operation from a distance in order to learn the combination. The face plate is the visible part of a lock and therefore the weak link if somebody is observing the area. Yet another option is to eliminate the latch hold-back feature so that the lock can never be kept open. It will then remain locked at all times, except for a brief moment when the correct combination is used.

Certain locks will also allow two push buttons to be pushed at the same time, in effect producing a different number, in order to raise the security level. However, these locking units cannot use the same push button more than once in a given combination.

The majority of the push-button locks work in the following way. First turn the control knob to the left to activate the push buttons. Then press the push buttons in the correct combination. Finally, release the last push button or push buttons before turning the control knob to the right. This will open the lock. The lock can then be relocked by turning the control knob to the left, or, alternatively, relocking will be an automatic feature.

The lock cannot be opened by removing the control knob, as this knob is connected to the lock by a friction clutch. The internal mechanism of the lock will therefore be damaged if the control knob is forced or removed.

Other push-button combination locks employ four-digit or seven-digit combinations. In these locks, there are usually ten push buttons to choose between. These units can frequently be unlocked by either a four-digit change combination or a six-digit master combination. The master combi-

nation might work for several different locks in exactly the same way as a master key. Although these locks may be electronic, they are often mechanical. We will deal with electronic locks in more detail in Chapter 6.

Sesame locks (fig. 26) are extremely simple combination locks that are frequently found on briefcases and suitcases. These consist of three dials numbered from zero to nine. The number of possible combinations is very low—only one thousand. This means that the correct combination can

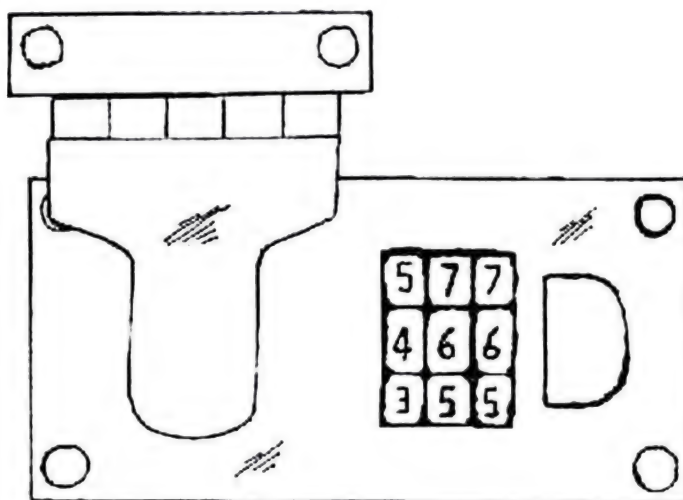


Figure 26. Sesame combination lock.

be found by trial and error if sufficient time is available. Expect to spend about half an hour to go through all possible combinations. Less time is usually enough, as the correct combination is often found long before you have checked all of them.

Begin the process by setting all three dials to zero. Then move dial C to 1, 2, 3, 4, 5, 6, 7, 8, and 9, one after the other, while pressing the catch after each change in number. Unless the correct combination has been found, change the setting of dial B to 1. Dial A will remain on zero. Once again, repeat all numbers on dial C while pressing the catch as before. If the correct combination has not been found, set dial B to 2, and repeat the process. Continue the process until dial B has been set to all possible numbers. Then set

dial A to 1 and repeat the entire operation once again. Dial A is then set to 2, and the process is repeated.

This process, although boring, is in fact easy to perform and will sooner or later result in the lock being opened. Do not try to think of what you are doing; simply learn the process by rote and do it.

Combination padlocks with a dial can be opened in basically the same way as other dial-type combination locks, but they are usually simpler in construction and are consequently easier to open. For this reason, they are often used for practice. Remember, though, that it is easier to locate the gates within the combination padlock if you pull out the shackle as you rotate the wheels. It is also easier to open combination padlocks that have been in use for a long time because the gates on the wheels will have become smoothed down, which will simplify the manipulation of the wheels.

Yet another type of combination padlock is the sesame padlock (fig. 27). This padlock has no dial but works instead on the same principle as the sesame lock described above. However, the sesame padlock has four combination wheels, numbered from zero to nine. The method used to open a sesame lock with only three wheels is therefore not very practical on this padlock, as the required time to check all possible combinations would be approximately ten times as long, or five hours. There is, however, another way to open this lock.

The four-wheel sesame padlock is designed to unlock the

shackle only when each wheel is positioned so that a flat spot on each wheel is aligned with the corresponding flat spots on the other wheels. Each wheel

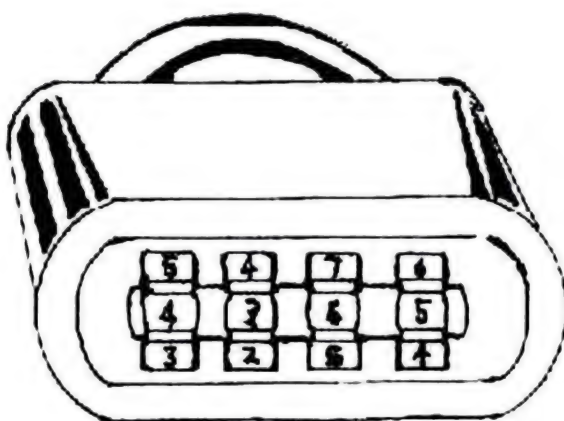


Figure 27. Sesame padlock.



Figure 28. Manipulating the sesame padlock.

has a changeable hub with such a flat spot. These flat spots, when aligned toward the side of the lock stamped with the trademark, will unlock the padlock. The current combination of the padlock determines where the flat spots will be located on the wheels.

A special tool (fig. 28) made of very thin steel can be used to locate these flat spots. Insert the tool into the lock between the wheel and the housing. Turn the wheel slowly and try to locate the flat spot. When it is found, either add or subtract five from the indicated number. This will give the correct combination number of that wheel.

Another, not very obvious type of combination lock is the remote-control lock. Such a lock is activated by an infrared beam from a hand-held device. Remote-control locks are generally used only on garage doors and driveway gates. Although the signal opening the lock is supposed to be unique, these locks are not very secure. This makes no difference, as these devices are never used to protect really important positions. See Chapter 6 for more information on remote-control locks.

PADLOCKS

The padlock was first invented by the ancient Romans. Today a variety are in common use, including warded, lever, disc tumbler, pin tumbler, and combination types.

Padlocks can usually be picked quite easily. Hold the padlock with the same hand with which you are using the torque wrench. It is generally easiest to do this by holding the padlock between the thumb and the forefinger. Then you can hold the wrench with your ring and little finger.

Your main hand is then free to work the lock pick. Take some time practicing how to hold the padlock, though, and make certain that it is easy to work on it. Different people sometimes prefer to hold the padlock in different ways.

Padlocks are not really that different from standard locks of the same type. Some smaller and simpler warded padlocks, for instance, have a single ward only and take very simple keys. Otherwise they are designed in the same way as other warded locks. The majority of the warded padlocks have three wards, or at least two. The key must pass through the wards before it can disengage the spring bar from the slot in the shackle end.

A warded padlock can be defeated by a skeleton key.

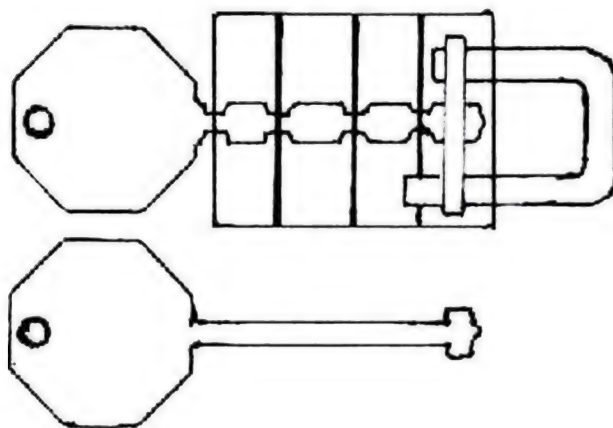


Figure 29. Warded padlock with the internal wards illustrated and a suitable skeleton key.

This is an ordinary key, but it is ground down (fig. 29). Note that skeleton keys are illegal in many locations. There are a few basic shapes, one of which will almost certainly defeat the lock. See the first section of this chapter.

Most warded padlocks can also be picked with an improvised T-shaped wire pick (fig. 30). Such a pick is easily improvised from a piece of stiff piano wire. An old method of picking padlocks is to insert a hat pin through

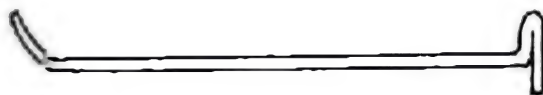


Figure 30. T-shaped wire pick.

the keyway and then use it to disengage the shackle bolt. This still works with older types of padlocks, but not with the recent, more secure ones. Warded padlocks can also be impressed easily. The procedure is the same as with ordinary warded locks.

The other types of padlocks, including the cylinder types, can be picked or impressed in roughly the same way as the ordinary locks of their type. Disc tumbler padlocks can also be picked, but it takes practice. Another possibility is sometimes, but not always, to acquire a set of test keys from a locksmith supply house. Such keys will facilitate the work.

Whenever picking a padlock, remember that in some padlocks you need to pull the shackle in order to help release it from the locking spring. If this does not help, repeatedly work the shackle in and out while picking the lock. This will unlock the mechanism eventually.

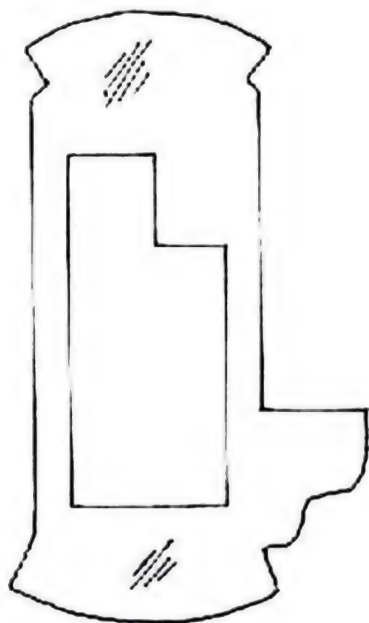
MASTER KEY SYSTEMS

Master keys can be made because a single key can be cut to match several lock combinations. Master keying always relies on coding systems that allow the locksmith to distinguish various key cuts and tumbler arrangements. In most key coding systems, the tumblers can be set to any of five possible depths. Since most locks have five tumblers and each one has five possible depth settings, there can be thousands of different combinations.

Warded locks and lever locks may also be master-keyed, but the security level will then be low. Disc tumbler locks, and especially pin tumbler locks, are more commonly used for this purpose.

Disc tumbler locks, when adapted to master-keying, are peculiar in that the master key will use a completely different keyway, located next to the regular one. This can be seen by closely inspecting the lock. The master key will operate on the left side of the tumbler, while the change key, the regular key, will operate on the right side (fig. 31).

Pin tumbler locks are master-keyed by adding another



pin, the master pin, between the top and the bottom pin in at least one pin chamber. The master key will have some cuts identical to the change keys, but it will operate the lock by raising the other pin or pins to the "new" shear line created by the master pin (fig. 32). What actually happens is that there will be two breaks for the shear line. In effect, this makes the lock slightly easier to pick, as

Figure 31. Disc tumbler prepared for master keying.

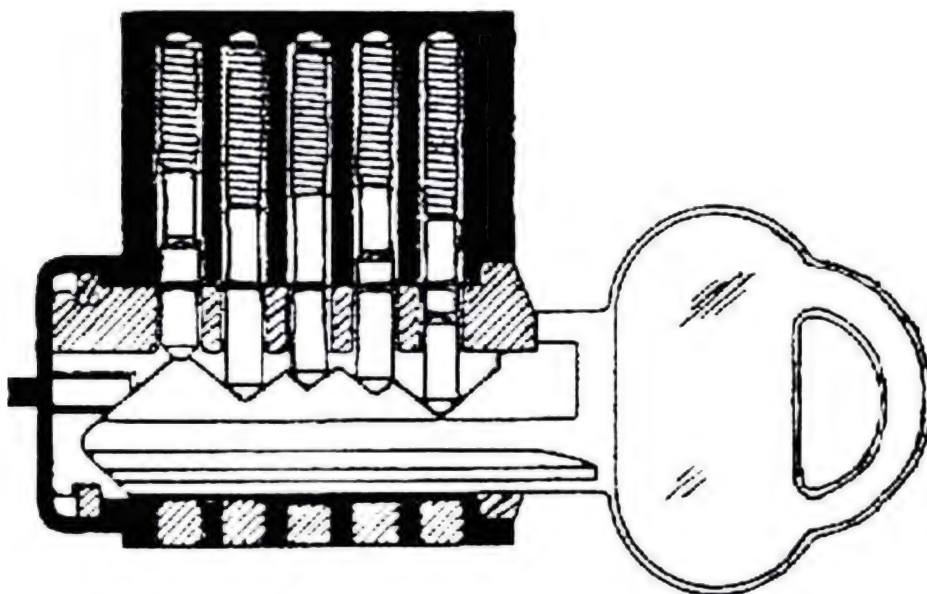


Figure 32. The master key relies on raising one or more master pin tumblers to a "new" shear line.

there are more possible combinations that will raise the pins to the shear line. In master-key systems with many different locks, there might be one or more such master pins between all regular pins. In this case, the system allows for numerous locks, and also several submaster keys. These systems are usually factory designed and

manufactured and can include as many as four breaks at the shear line.

A master key will not open all locks in a building, unless it is a so-called building master key or an emergency master key, which is a top-level master key that will operate all the locks at all times. It is more common to encounter, for instance, an engineer's key, which is a selective master key that is used by various maintenance personnel. It is therefore necessary to ascertain the level of the master key copied or otherwise obtained before it is used in an actual entry operation. In some low-security systems, the level might be stamped onto the key, although today it is more common to keep a master-key system chart in a safe place, detailing all the various key numbers and the key's position in the key hierarchy. The key will then only be identified by a code.

A master-key system is always divided into several different hierarchies, or key levels (fig. 33). If a master key can be obtained, it is advisable to identify its place within the hierarchy, as this will indicate which locks you can use the key in.

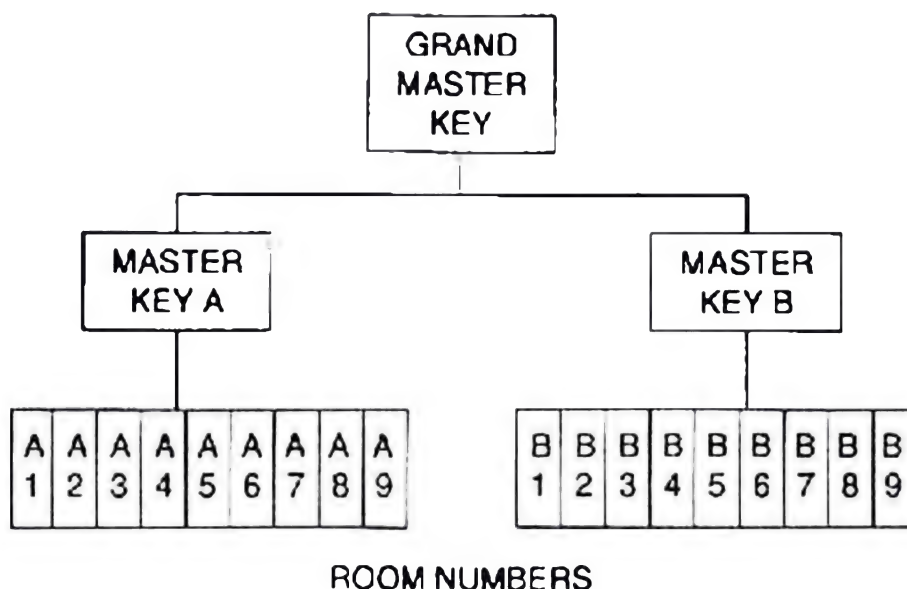


Figure 33. An example of a master key hierarchy.

Improvising Lock-Picking Tools

Picking a lock is not easy, and, with the exception of the simplest locks, it takes a considerable amount of time. It is therefore usually better to rely on an experienced locksmith to make a new key to the lock, especially if you have to enter the area protected by the lock more than once. He will then utilize the various impressioning techniques described in the previous chapter. However, in emergencies it might still be necessary to pick a lock.

A definite prerequisite for lock picking is a very good knowledge of the lock and how its mechanism works. It is also usually necessary to have the proper tools—lock picks—to do the job. Actually, a pick is not usually a special tool, but rather any device that is used to manipulate the tumblers in a cylinder into an unlocked position or to bypass whatever device is protecting the lock from being opened. Lock picks can therefore be improvised easily, as long as some basic materials and a few simple tools are available. Remember, though, that without a proper locksmith's license, the possession of lock picks is illegal in many locations.

It is not really necessary to carry lock picks on one's person except when they are definitely required. Lock picks can be made from easily obtained raw material almost anywhere, and the only essential tools are a pair of pliers and a

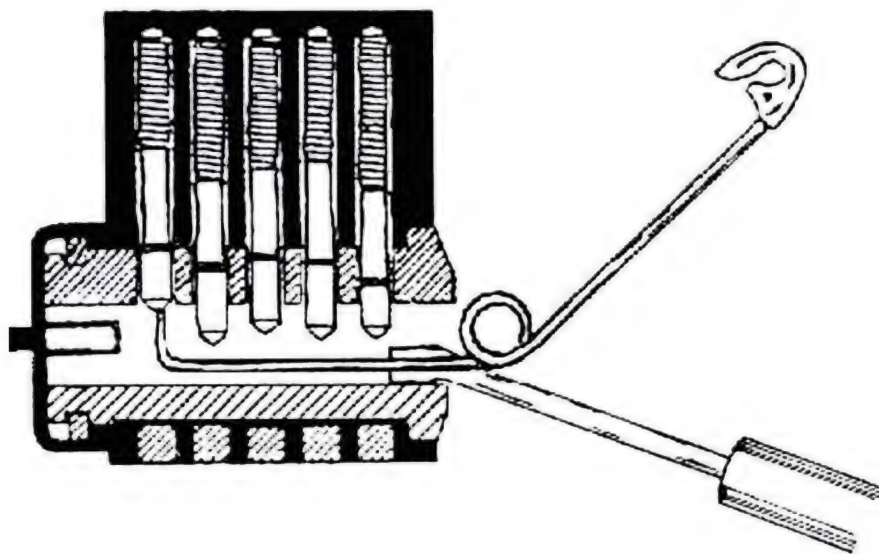


Figure 34. Picking a pin tumbler cylinder lock with a safety pin and a small screwdriver.

file. These tools, unlike the actual lock picks, do not gain the attention of the police or enemy if an operative who is in possession of them is searched.

In a real emergency, whatever is at hand can be used as a lock pick, although the work will then often be slightly more difficult. It is, for instance, quite possible to use a large safety pin and a small, slightly bent screwdriver instead of a pin tumbler lock pick and a torque wrench. Simply bend the tip of the safety pin at a 45-degree angle so that you can use it inside the lock (fig. 34). If no pliers are available, it is easy to bend the safety pin with the help of the keyway of the lock you are going to pick. The safety pin should be quite large, at least four centimeters long, so that you will be able to hold it easily while you are working on the lock. It helps if the tip is filed flat, as this will make it easier to locate and raise the pins.

"Real" lock picks come in numerous shapes, depending on the type of lock to be picked (fig. 35). Lock picks can be made easily from flat, cold-rolled steel that is less than half a millimeter to a little less than a millimeter thick. The actual thickness is really not very important, except that the pick must be able to enter the lock and work in there. The

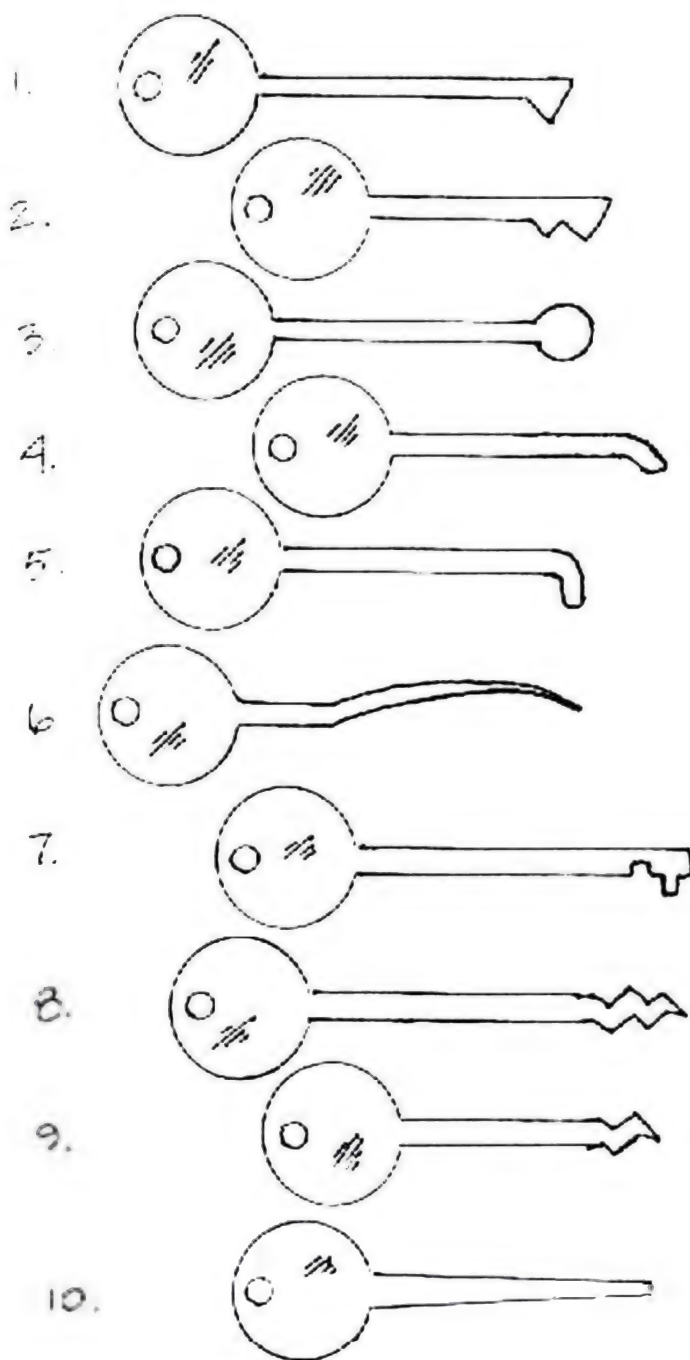


Figure 35. Various types of lock picks: 1. diamond lock pick, 2. double diamond lock pick, 3. circular or ball lock pick, 4. half-round feeler lock pick, 5. round feeler lock pick, 6. reading tool, 7. flat lever lock pick, 8. rake, 9. half-rake, 10. tubular cylinder lock pick.

steel strip should be about 15 centimeters long and at least 8 to 10 millimeters wide. Some people prefer to have one end fitted with a handle, while others prefer their lock picks to carry working surfaces on both ends.

Make your lock picks by grinding down the steel strips to the correct size with a file (the best option) or a grinder and a carborundum wheel. If the latter is used, take care that the metal does not become too brittle because of excessive heat.

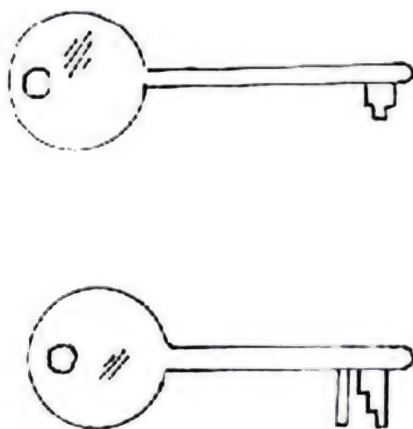


Figure 36. Lock picks for warded locks.

As was mentioned in Chapter 2, you will need lock picks of slightly different design for warded locks (fig. 36). These picks are easy to make. In many instances an old pre-cut key, ground down to pass the wards in the key-holes, is quite sufficient. Then it will in effect become a skeleton key.

One of the most useful lock picks is the diamond pick (see fig. 35). It can be used for most pin and disc tumbler locks. Most experienced locksmiths seem to use this pick much more than any other. It is really an all-around lock pick.

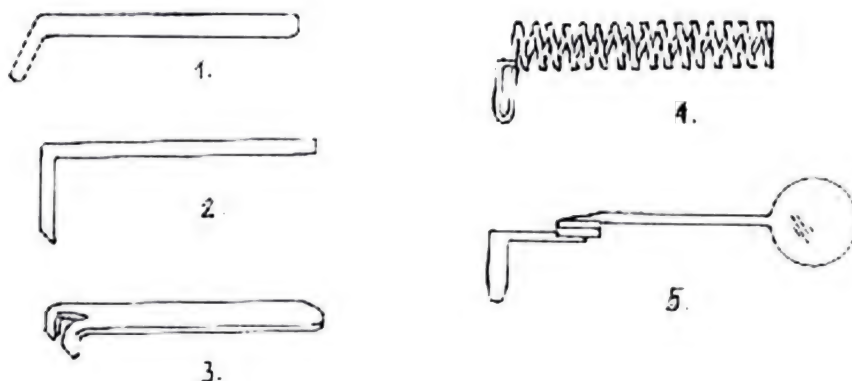


Figure 37. Torque wrenches: 1. & 2. basic torque wrenches, 3. torque wrench for double-sided disc tumbler locks, 4. & 5. steel spring torque wrenches.

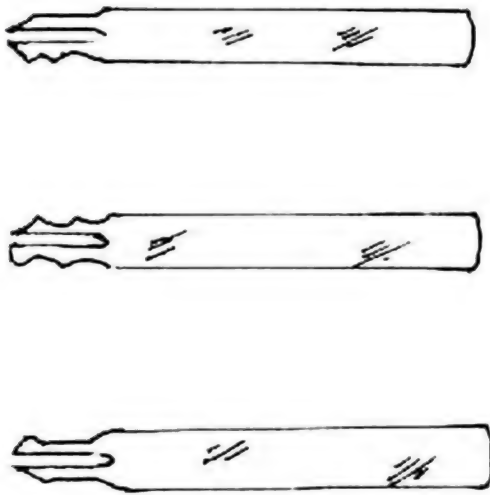


Figure 38. Lock picks for double-sided disc tumbler locks.

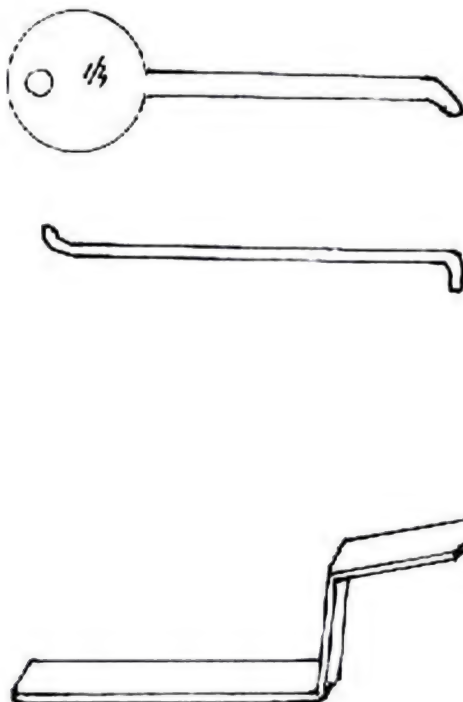


Figure 39. L-shaped lever lock pick, the same pick improvised from wire, and a suitable torque wrench.

Usually some kind of torque wrench must be used with the lock pick. These tools are made of hardened spring steel, around 7.5 to 12.5 centimeters in length and a little more than a millimeter thick. Sometimes longer torque wrenches are required, as these tools must be long enough to reach the interior of the lock. There are numerous variations, but the two most useful ones are the basic torque wrench and, for the really delicate work, the steel spring wrench (fig. 37).

Certain locks (double-sided disc tumbler locks, for instance) require special torque wrenches. Such picks and wrenches are more difficult to improvise (fig. 38) but can be acquired from a locksmith supply house.

The L-shaped lever tumbler lock pick can be made from spring steel no more than 2 to 3 millimeters thick. A torque wrench of the same thickness is also useful (fig. 39). Some individuals use a rake pick. As

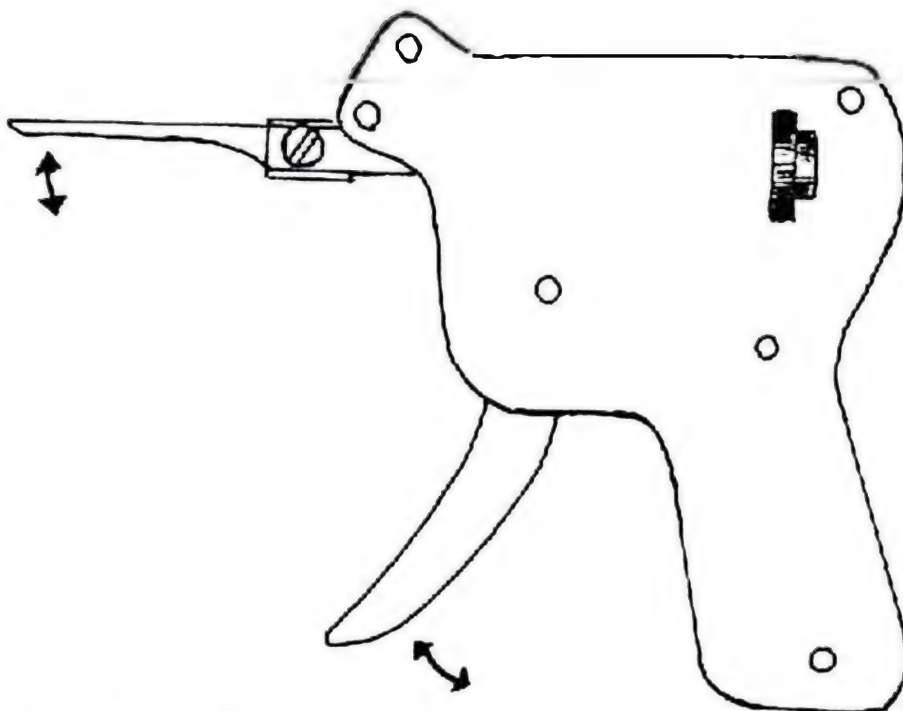


Figure 40. Pick gun.

was previously mentioned, such a pick is not very useful. If a rake pick really is desired, you can just as well use an ordinary diamond pick (see fig. 35) for the same purpose. Although some people make a living from manufacturing and advertising numerous types of lock picks, remember that it is not really necessary to have them all. In most cases, a simple pick will be sufficient. An operative who cannot pick a lock with a diamond pick is usually no better off with any other type of lock pick.

Finally, the device known as a pick gun (fig. 40) should be mentioned. This is a hand-held device that can be used to bounce the driver out of the plug in a pin tumbler lock and into the cylinder case. No great skill is required in order to use a pick gun, but this device is not necessarily faster, nor even better, than picking the lock manually. The pick gun cannot pick all types of locks and is therefore of more limited value than an experienced locksmith. The only time the pick gun might be really

useful is when you are picking a lock equipped with mushroom or spool drivers.

The pick gun is inserted into the keyway so that its pick is barely touching all the bottom pins. When the trigger is pressed, the pick gun will rap the pins up to the shear line so that a turning force can allow the plug to rotate and the lock to open.

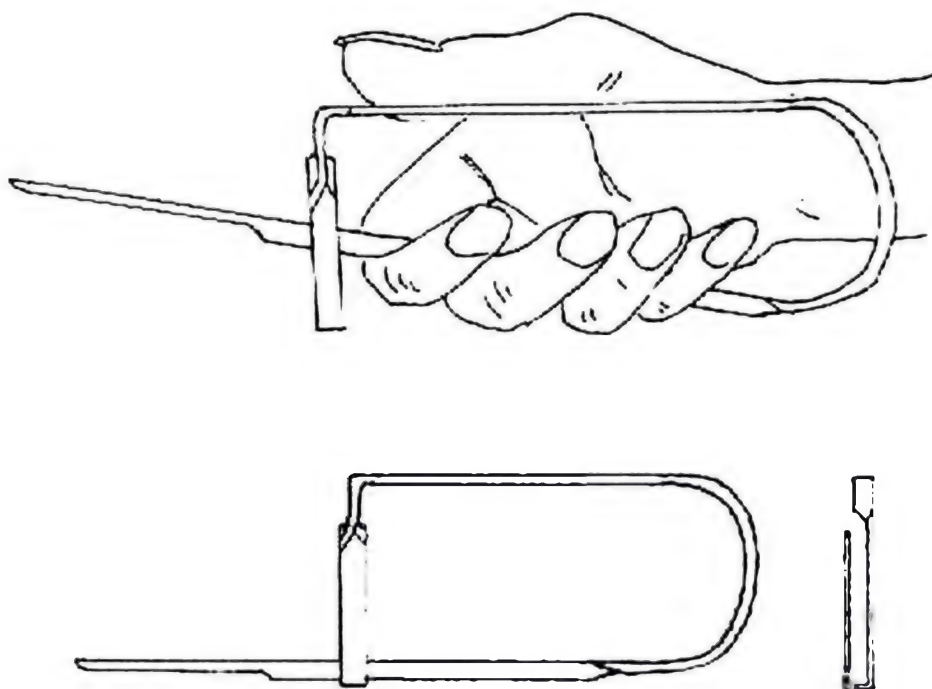


Figure 41. Snap pick.

There is also a manual version of the pick gun. This is known as a snap pick (fig. 41) and can be made easily from spring steel. Just as with the pick gun, insert the pick portion of the device into the keyway and hold so that it is just touching the bottom pins. Then press the upper part down with your thumb before quickly releasing it again. This will rap all the bottom pins. As these pins remain relatively stationary, the force will be transferred to the drivers, which are forced to move upward, compressing the spring. As the area at the shear line will then be open for a split-second, a slight turning force will allow the plug to rotate.

The principle of both the pick gun and the snap pick is

illustrated easily by the fact that force will be transferred through stationary matter. This can be seen in an experiment with three coins on a table. If the coins are lined up touching each other and the coin in the center is held firmly to the table with a finger, the coin on one side will move if the coin on the opposite side is pushed to strike the stationary center coin. The momentary force will be transferred through the stationary coin and instead move the opposite coin. In the same way, the drivers will be moved by the force applied to the bottom pins.

When working with a pick, always remember to use the narrowest pick you have available, as this will give you maximum working space. The pick should be held in about the same manner as a pencil. No wrist action is desired, as only the fingers are dexterous enough to manipulate the pick inside the lock. Wrist action will only make you tired. Lock picking is not a matter of physical strength.

It is also helpful to steady your hand by placing your little finger against the door when you are working on the lock. If the lock is a key-in-knob cylinder, however, steady your hand against the edge of the knob instead.

The pick should be able to enter the keyway above the torque wrench without moving any of the tumblers. If this is impossible, then the torque wrench is either too high in the lock or the keyway grooves are such that the torque wrench must go in at the very top of the keyway. In these cases, picking the lock will be difficult.

Despite the control apparatus established in order to make sure that only professional locksmiths get hold of lock-picking tools, there are various ways of acquiring them. Most manufacturers and distributors of locksmithing equipment refuse to do business with anyone but professional locksmiths. However, they are quite satisfied to send their products by mail to anybody who can prove in any way that he has these qualifications. I say "in any way" because I have found out that a fancy letterhead, business card, or photocopy of a forged locksmith license is usually enough. A photocopy of your advertisement in the Yellow Pages will also be accept-

able as proof of professional status. After all, money does not smell!

Many lock-pick sets, both commercially available and improvised ones, are designed to be hidden in various objects so as not to compromise the user. One popular design hides the picks inside a pen cover or in the handle of a hobby knife. In the latter case, the hobby knife can also be used as a handle for the pick, making it easier to hold. A lock pick set might also be hidden inside a jackknife handle or in any other suitable location; the only limit to the possibilities is the operative's imagination.

As a final point, always remember that a real key is quicker and safer than any lock-picking skills. Even if it turns out to be impossible to acquire one of the keys to the building you need to enter, there might be ways of at least inspecting the original key. If a key can be handled for some time, even if it cannot be taken out of the building, it is almost always quite possible to make an impression in wax or a full-scale drawing, and then make a copy at a later time.

Naturally, the full-scale drawing must be done with extreme care, including detailed measurements of every part of the key. This is generally easy, although tedious, except when it comes to the diameter of the key. In certain types of locks, the diameter can often be measured instead by wrapping a paper clip around the original key. The paper clip can then be taken out of the building. In this way, the need for special equipment for measuring the key is avoided.

Other Means of Illegal Entry

WINDOW ENTRY

There are various ways of opening an unlocked window from the outside, depending on the type of the window. The easiest one to open is the sash window. This consists of two halves, the top and the bottom, that slide up and down. The latch is located between these two halves. One of the oldest

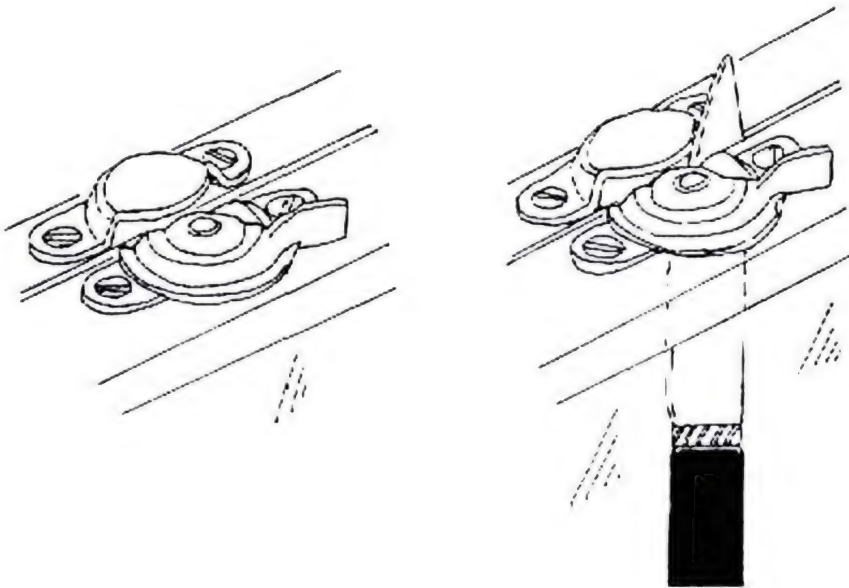


Figure 42. Opening an unlocked sash window from the outside.

tricks of the trade is to slip a knife shim or similar device up between the sashes, or upper and lower halves of the window, to move the window latch to the open position (fig. 42). The window can then be opened easily.

If the area between the window halves is too narrow for a knife, then you can drill a narrow hole at an angle through the wood molding to the base of the latch, insert a stiff wire through the hole, and push the latch back. Hide the hole with paint or dirt afterwards. Unfortunately, contemporary fasteners cannot be manipulated in this way. The fitch fastener, for instance, is a pivoting device with a snail-like cam that cannot be knocked back. The Brighton fastener, another type, relies instead on a screw-down acorn that clamps the sashes together securely. These fasteners also sometimes contain integral locks.

Sometimes the upper and lower window half, or sash, will be connected by means of a bolt slipped into a hole drilled through the lower sash and partially into the upper sash. This was commonly done in older buildings to conserve energy as well as increase the security of the window. If this is the case, simply drill a small hole to the bolt and

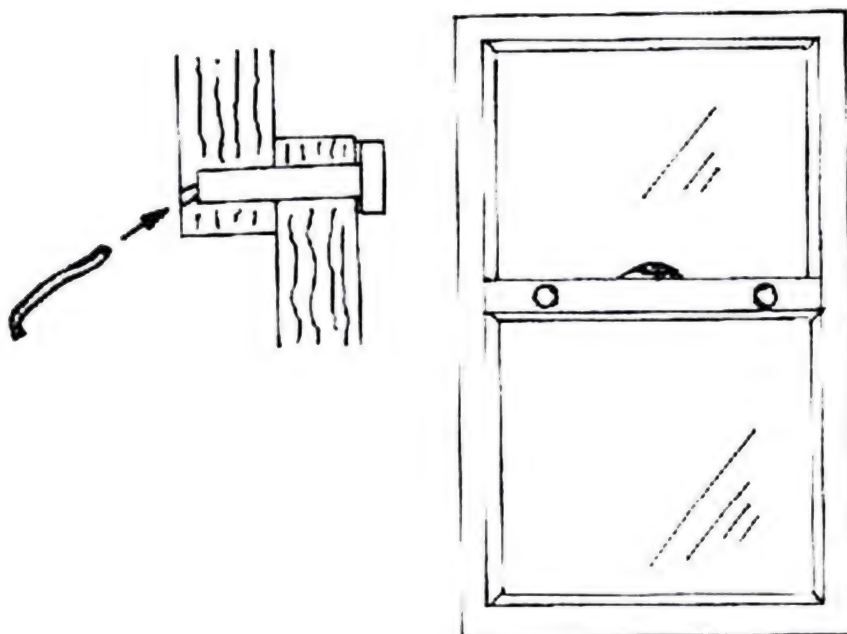


Figure 43. Opening a bolted sash window from the outside.

then push the bolt out of the upper sash with any pointed object, such as a nail (fig. 43). The small hole will usually be difficult to see, and it, too, can be hidden with putty, paint, or dirt.

Other types of windows can also be opened from the outside if a narrow hole is drilled in order to allow a piece of wire to be inserted. Unfortunately, these holes must be drilled in locations where they are much more likely to be noticed by the inhabitants of the house. Another complication is that the windows might be locked. All windows, including sash windows, can be fitted with locks. These come in various types, but all of them are of fairly simple construction. This is of little help, however, as the locks are impossible to open from the outside except by breaking the window.

TRANSOM ENTRY, DOORS, AND DOOR CHAINS

Picking a lock is not the only means of entering through a locked door. There are various other methods, most of which have been in use for quite some time. There are, for instance, ways of entering through a transom and ways of entering by manipulating the lock construction without actually picking the lock.

If a door warbles slightly and the lock is of an older construction that lacks a deadlocking function, the bolt can be retracted with a celluloid strip by the process known as "loiding." This process involves slipping a flat object between the bolt and the strike. The strike, or striking plate, is the part of the locking arrangement that receives the bolt, latch, or fastener. It is recessed in the door frame. A little pressure might allow space enough to insert a celluloid strip between the lock and the striking plate. Then only a slight pressure on the inserted celluloid strip will force the latch back and release the lock. This will open the door.

The door might, however, be fitted with a so-called antipick latch. This is a spring latch fitted with a parallel bar that is depressed by the strike when the door is closed. The depressed bar will prevent the latch from responding

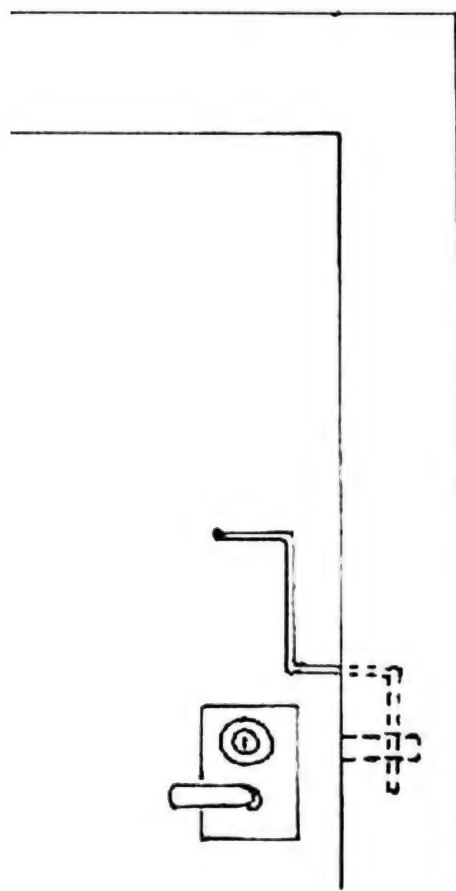
to external pressure of any kind. This naturally makes loid-
ing impossible.

A variation of this method is to insert a thin knife, a
linoleum one, for instance, between the door and the jamb.
The knife's point should be tipped upwards. Then insert a
pry bar above the linoleum knife in order to spread the
door slightly. Then the latch can be disengaged. Bring the
linoleum knife forward, push the latch bolt back into the
locking assembly, and open the door. Of course, if there is
sufficient space between the door and the frame, the
linoleum knife alone is sufficient to move the bolt back.

If, however, there is no space to insert a pry bar, wooden
wedges must be used. One wedge should be inserted on
each side of the bolt, about 10 to 15 centimeters away from
the bolt assembly. This will spread the door away from the
jamb sufficiently to insert the pry bar.

Modern doors and jambs sometimes fit so well that it is
impossible to even insert a
wedge. In this case, a
stainless-steel shim can be
used. Force the shim into
the narrow crevice be-
tween the door and its
frame and attempt to push
the bolt back.

Another way of open-
ing a door is to use a so
called Z-wire (fig. 44). This
is a tool made from a stiff,
thick wire, 25 to 30 cen-
timeters long. Insert the Z-
wire between the door and
the jamb until the short
end is all the way in. Then
rotate it toward you at the
top. This will cause the



*Figure 44. Opening a door with
the Z-wire.*

opposite end to rotate between the door and the jamb, contacting and hopefully retracting the bolt. When the bolt binds, exert pressure on the knob to force the door open.

Another problem sometimes encountered is a locked door chain. When you have managed to open the door, you will find that the door chain prevents the door from opening fully and that you cannot reach the chain in order to remove it. Fortunately, you can solve this problem by removing the chain with a rubber band. Reach inside and stick a tack in the door behind the chain assembly. Attach one end of the rubber band to the tack and the other end to the end of the chain (fig. 45). Make certain that the rubber band is taut. Then close the door, taking care not to lock it again. If this is difficult, secure the lock with adhesive tape so that the mechanism cannot work before you close the door.

When the door is closed, the rubber band will pull the chain back. If it is not completely pulled off the slide, shaking the door a little should do it.

The rubber band method is effective and easy to use, but it leaves an undesirable mark that can be seen easily on any well-kept door. It is then much better to use a bent coat

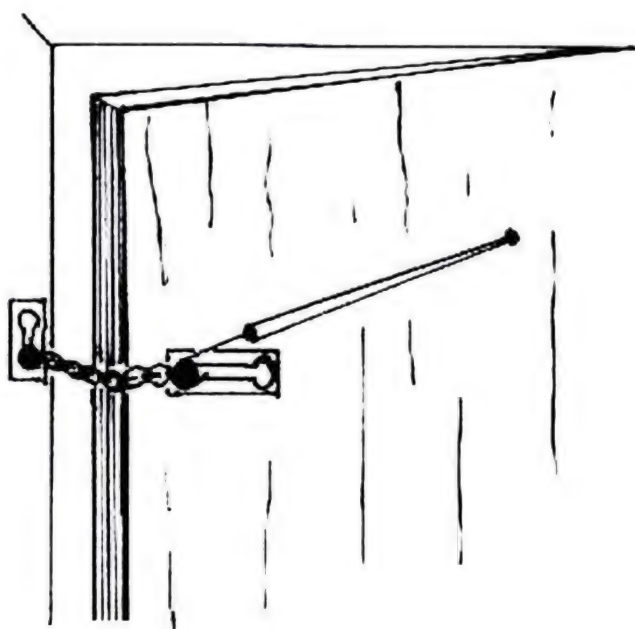


Figure 45. Unlocking a door chain with a rubber band and a tack.

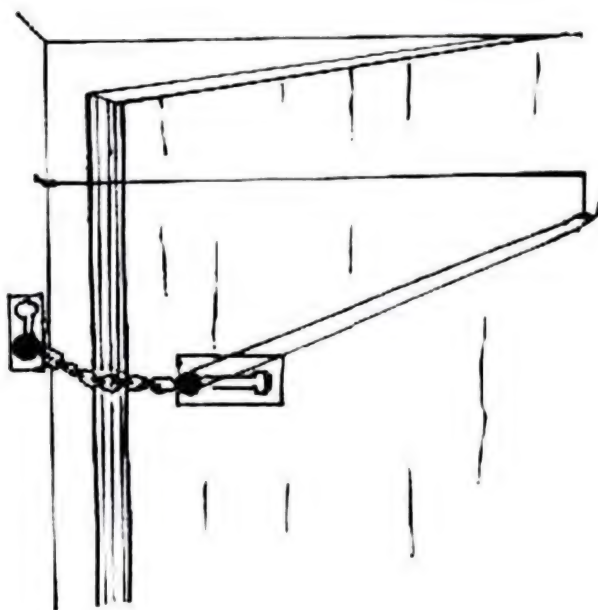


Figure 46. Unlocking a door chain with a rubber band and a bent coat hanger.

hanger to stretch the rubber band (fig. 46), rather than a tack. The coat hanger must be properly bent and long enough so that the door can be closed as far as possible.

An even easier method that can be used on doors with large enough space between the door and the jamb is to insert a thin wire to move the chain back.

If a transom has been left open or unlocked, there are a number of ways to enter. If the transom is completely open, simply crawl through, stepping on the door knob if necessary. If the transom is only partially open, however, it might be impossible to crawl through. Then lower a length of cord through the transom to form a loop which, when wrapped and drawn taut around the inside doorknob, might twist it enough to open the lock if you draw upwards on one of the two ends (fig. 47).

It is often easier to use two long pieces of string connected by a strip of rubber inner tubing or an electric cable covered by a strip of rubber than to use ordinary cord. The tubing should be 20 to 25 centimeters long. It is possible to open both a regular door knob and an auxiliary latch unit

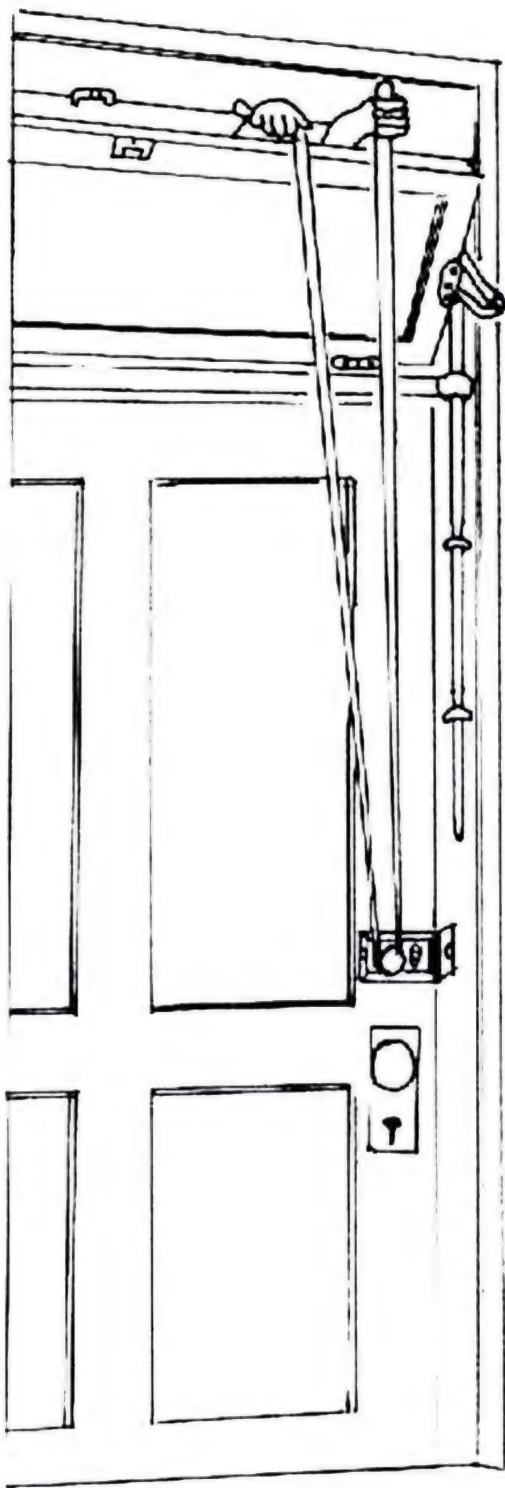


Figure 47. Transom entry.

with this method, as long as a key is not required from the inside as well.

Yet another means of covert entry is to gently pry loose the molding around one of the door panels with a thin, flat chisel. If the panel can be removed without damaging it, the operative can crawl through the opening or at least reach through it and release the lock in the door.

It is also possible in some cases to open a door simply by bending it open by spreading the door frame. This can be done unless a very long bolt is used or the frame is very rigid. Take care that the door is not damaged, however, as this happens easily.

In certain countries, especially tropical ones, doorsteps are not very common. It might then happen that the owner of the house locks his front door from the inside and then leaves the key in the lock. An old but still reliable trick is to insert a paper sheet, an old newspaper, for

instance, under the door. Then push the key out of the keyway with a wire. As the key falls down and lands on the piece of paper, you can easily pull both paper and key back and then use the key to open the door.

FILE CABINETS AND DISK DRAWERS

There are various ways to open file cabinets and desk drawers, so you have to determine the best method based on the construction of the cabinet or drawer and the type of lock used in the object. With the exception of most sliding cabinet doors, however, the design is more or less standardized.

File cabinets are found in most offices. The locking device of such a cabinet relies upon a bolt that extends from the top of the lock body. The bolt manipulates the control bars that lock each drawer of the cabinet in place. As the bolt is spring-driven, it will extend out of the lock at all times, unless the lock plug is turned. The plug has a cam attached to the back, which rotates in conjunction with the plug. This cam works in a notch on the side of the bolt, thus operating the bolt (fig. 48). The cam can also be the actual lock bolt, especially in many drawer locks.

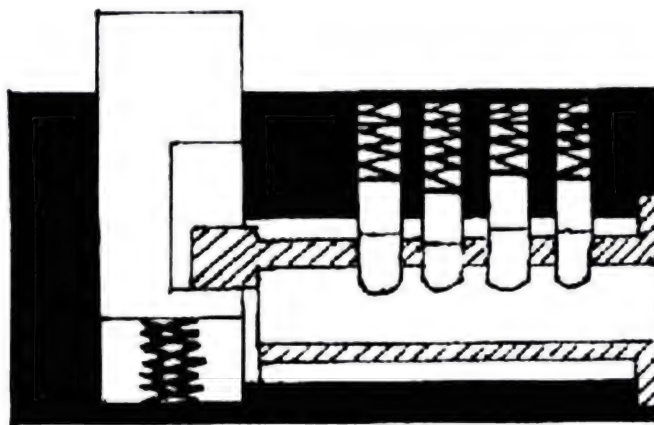


Figure 48. The cam of the plug operates the bolt in most file cabinets.

Locks of this type are generally not very secure. They usually have open keyways, with the keyway running from the face all the way through the body of the plug. This means

that the lock can be opened most easily by jimmying. A jimmy is a pointed tool made of a thin strip of spring steel 3 to 5 millimeters wide. Slip the jimmy through the keyway and manipulate the bolt directly, pulling the bolt downward, without bothering to actually pick the lock (fig. 49).

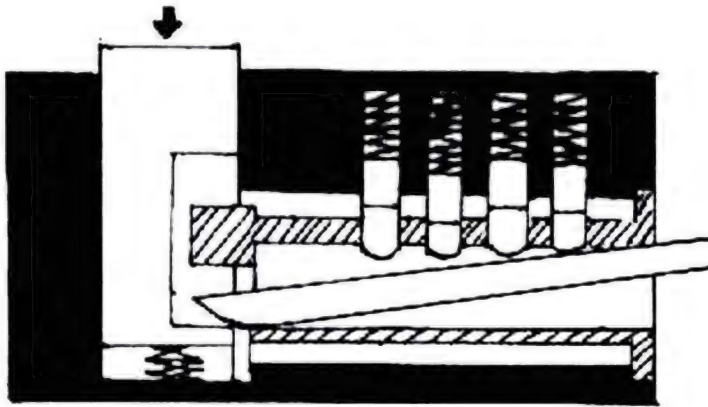


Figure 49. Pulling down the bolt with a jimmy.

Some contemporary locks of this type do contain some kind of protection against jimmying the lock open. For instance, the keyway might be blocked by a piece of metal or a pin so that no access to the bolt is allowed. These locks must be picked, or, alternatively, a rod of stiff wire not more than 5 or 6 millimeters in diameter and at least 30 centimeters long, with one end turned 90 degrees, can be inserted between the drawer and the cabinet face. The bolt mechanism can then be forced down with this wire (fig. 50). The rod should be turned counterclockwise in most cases.

Yet another method also involves prying the drawer open with, for instance, a thin piece of string steel or a wedge, far enough to allow direct manipulation of the bolt. A strip of steel, about 45 centimeters long and between 1 and 2 centimeters wide and 1/2 millimeter thick, or even an ordinary letter opener, can then be used between the drawer catch and the bolt mechanism to pull the drawer open. The opening tool will create a bridge for the drawer catch of the mechanism to ride upon and pass the bolt (fig.

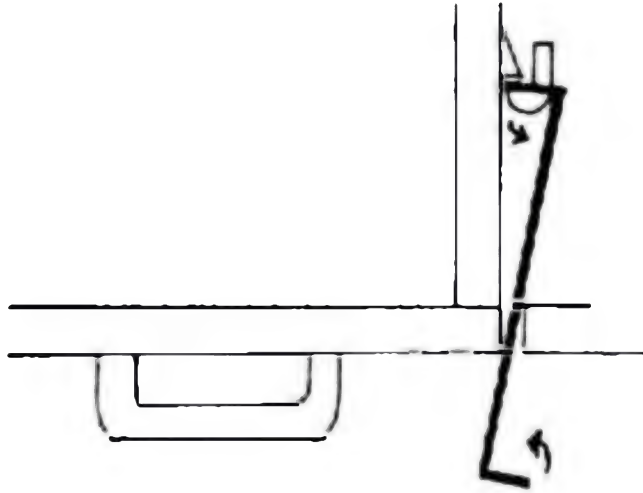


Figure 50. Forcing the bolt mechanism down to release the drawer catch.

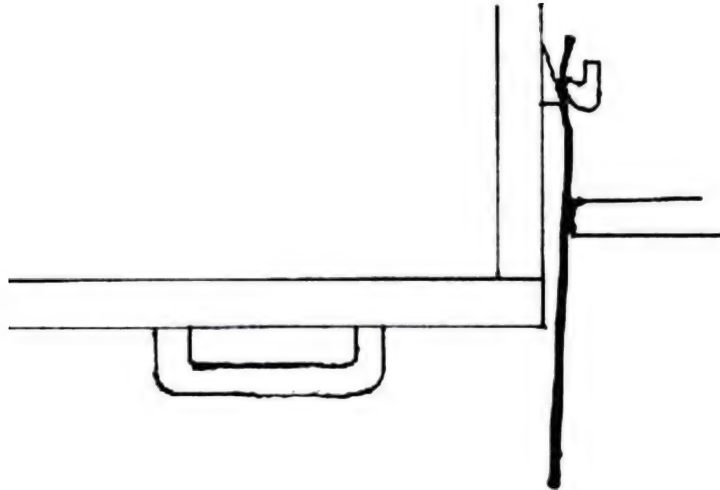


Figure 51. The drawer catch passes the bolt mechanism, riding on an inserted strip of steel.

51). Usually you must pull quite hard. Older types of file cabinets can be opened by simply spreading the file cabinet from its frame with a screwdriver, while a thin but strong tool, say a hacksaw blade about 30 centimeters long, is inserted in order to lift the bolt mechanism away from the drawer catch.

Certain types of file cabinets function in the same way, but with the mechanism effectively out of reach, hidden in

the rear portion of the cabinet. Then it is sometimes possible to tip the file and in this way gain access to the mechanism, forcing it upward to release the drawers. If the cabinet is designed in this way, the mechanism can be seen protruding through the bottom partition of the cabinet.

Yet another method, one that works with certain types of file cabinets, is to tilt the cabinet backward about 15 to 20 centimeters off the floor and then suddenly release it so that one drawer catch will disengage itself from the catch on the mechanism rod. The drawer will then be released, and the operative will be able to open the remaining drawers by hand. Simply reach inside the cabinet and release the rod that keeps them in the locked position.

Certain file cabinets instead have gravity-type vertical engaging bolts. These can be released most effectively by inverting the entire structure.

Although most file cabinets have the lock in the same position, there are various ways of arranging the locking bar and locks in a group of desk drawers. This makes it important to choose the best way when it comes to opening a drawer. If all other methods fail, it is always possible to pick the lock itself. The best option, of course, is to find an identical cabinet and practice on it before the actual operation takes place.

Desks with locking drawers controlled from the center drawer can be opened in another way. Many of these are constructed so that there is a space between the back panel of the desk and the back of the desk drawers. The locking bar is usually designed to engage the desk by either upward or downward pressure. Whether it is upward or downward will depend on the style of bolt used in the design. The spring-loaded bolt will be pushed automatically into the locked position by the motion made when the locking drawer is closed. To open the side drawers, the operative must push the bolt up by hand from under the desk, reaching up between the back panel and the back of the desk drawers. When the bolt is raised, the hook catches will be released and the side drawers can be opened. The center drawer will

have its own lock, of course, which might have to be picked open.

Other types of desks might require the use of a little force coupled with pulling outward on the center drawer. This will push the bolting mechanism downward just enough to open the various drawers.

The center drawer lock can be opened in the following way. First insert a screwdriver or another prying tool between the drawer and the underside of the desk. It might be necessary to protect the underside of the desk from scratching with some cardboard or thick tape. Then pry the drawer away from the desk top. Now use another, similar tool to pull the drawer outward to open it. Be careful, though, as this process might damage the drawer.

A final way of opening the lock, which is not really recommended as it will leave clear traces of the attempt, is to drill a small hole in the drawer above the lock. Insert a stiff piece of wire, such as a paper clip, into the hole to push down the plug retainer ring. This will pull the plug free of the lock, which will cause the bolt to drop down into the open position. The resulting hole can be partially hidden by inserting a wooden plug of the right material, but it will always be revealed by a careful investigation.

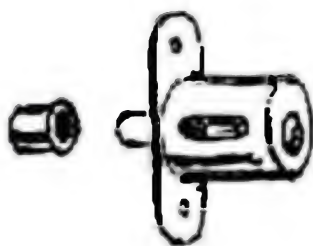


Figure 52. Sliding cabinet door plunger lock.

A sliding cabinet door is often locked by a plunger lock (fig. 52). Such a lock is mounted on the outside door. The bolt is a projection from the rear of the plug unit that engages a hole in the other sliding door of the cabinet. Neither door can then move, as they are locked against each other. The plug will be returned to the open position when the correct

key is inserted into the lock and turned. The actual lock will be either a disc tumbler lock (in old buildings) or, more commonly, a pin tumbler lock. The easiest way to open these locks is to spread the two doors far enough apart to disengage the bolt. Alternatively, the lock can be picked in the ordinary way.

VEHICLE DOORS, WINDOWS, AND TRUNKS

There are numerous ways of entering the average car. The door windows, the front and rear ventilation windows, the doors, and the trunk are all possible entrances. Sometimes the locks will be easy to pick, while at other times it will be easier to use some other method of entry. In this chapter we will look at some of these other methods. The methods used for picking the locks are described in Chapter 2.

The most vulnerable parts of the car are usually the windows. One reason for this is that most windows allow the door release push-button lever to be reached easily. This is especially true for the contemporary car models that have a single pane of glass. You can most easily reach and lift the push button with the help of a bent coat hanger. The coat hanger should be straightened out and then bent in a loop or a triangle on the end (fig. 53).

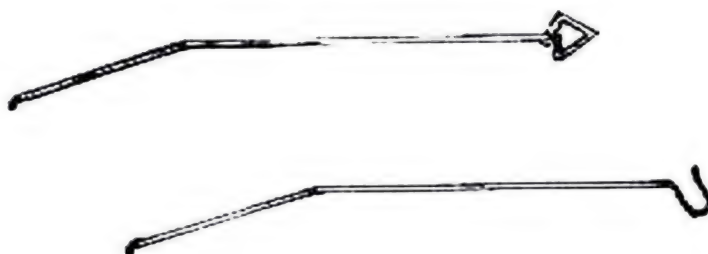


Figure 53. Coat hangers bent in loop and triangle.

First of all, as the window will usually be rolled up tight, force a paint scraper or a similar object between the edge of the window and the weather stripping (fig. 54). This will create an opening large enough to allow the coat hanger to be inserted in the resulting crevice. The loop or triangle can then be used to catch the push-button lever and pull it up. This will open the door.

Another possibility is to use a gun cleaning set instead of a coat hanger. As the gun cleaning set comes in sections, it is easy to make a rod long enough to reach across the inside of the car. In this case, always work on the window or door

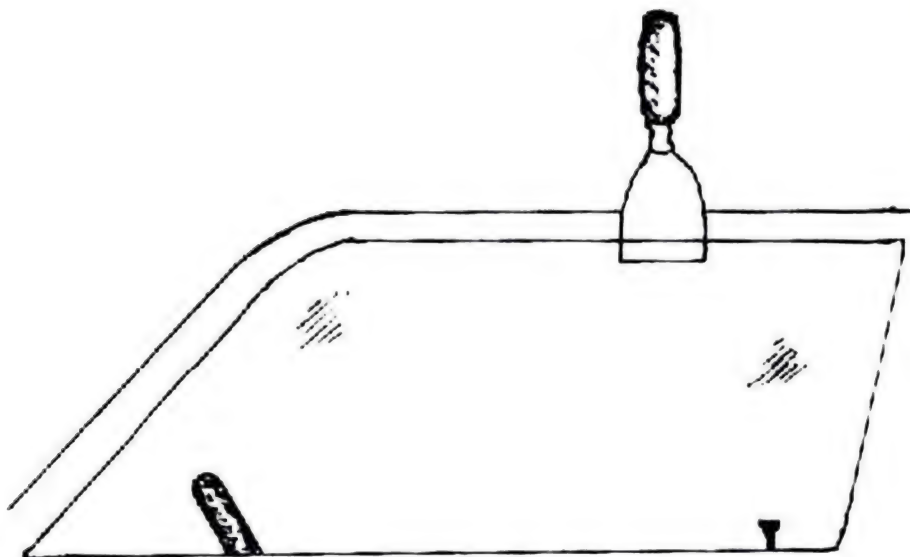


Figure 54. Paint scraper forced between the edge of the window and weather stripping.

opposite of the side where you insert the rod.

First of all, make a loop with some nylon line and fix it to the end of the rod on the slotted cleaning attachment included in the gun set (fig. 55). Then insert the rod and catch the lever or the door handle inside the car with the loop. Pull on the line and lift up the rod to raise the lever or

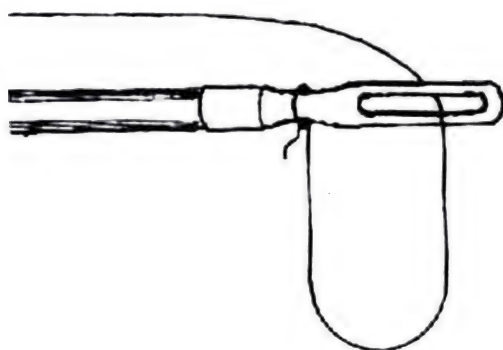


Figure 55. A loop of nylon line fixed to the slotted cleaning attachment.

the handle caught in the loop to the open position.

If the car has a rear ventilation or wing window, this can also be used to gain entrance. These windows come in two types—those with a locking button on the swivel and those without. If

there is no locking button, it is easy to force the swivel lock up and into the unlocked position. Simply insert a paint

scraper or a similar object between the window and the frame. Then bend the tool slightly in order to make an opening wide enough to allow a thin piece of wire through. Take care to loop this wire around the swivel level and then pull it upward. This is accomplished most easily if the wire is slightly bent on the end so that it does not slip off the lever.

The problem, however, is that most cars nowadays have locking push buttons in addition to the swivel levers. There are special tools available to take care of them. Two tools are required, and they are inserted on different sides of the lock. Depress the button by pulling the first tool toward you, while twisting the second one slightly to push the lever into the unlocked position (fig. 56).

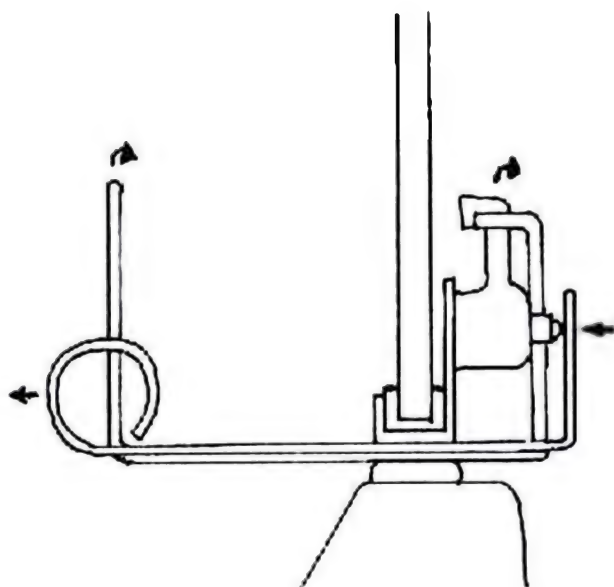


Figure 56. How to apply tools for opening rear ventilation windows with locking buttons.

The front ventilation window is another popular way of gaining entry to the vehicle. The reason is that it allows access to both the door handle and the window roller handle. Here, too, special tools are available that are very simple to use. Only pry the

window slightly open, insert the tool, and turn the handle (fig. 57). Which type of tool is chosen generally depends on the amount of working space available, as their function is the same.

The trunk of the car is a completely different matter. As the same key is often used both for the door locks, the ignition, the trunk, and even the glove compartment if it is locked, it is often helpful to deal with all of these locks at

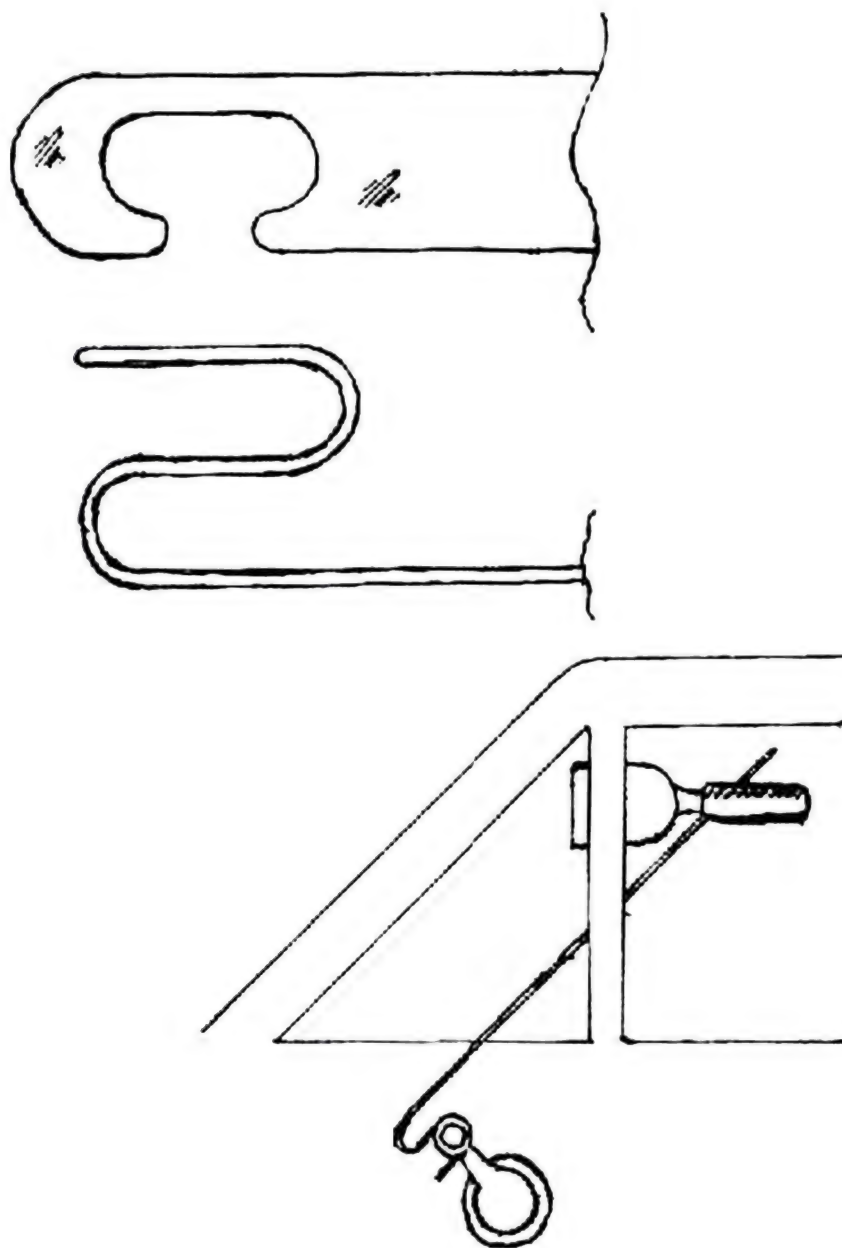


Figure 57. Tools for opening the front ventilation window.

the same time. Picking is the most common method of opening these locks, but it is often time-consuming. If you choose to drill the lock open, remember that many manufacturers have protected their locks by installing various steel plates or pins in front of the catch in order to make drilling more difficult. If drilling is required, it is often easi-

er to break the trunk open or to drill beside the catch lock and then manipulate the catch with a bent piece of wire. In either case, the intrusion will naturally leave very clear marks on the car.

A few trunk or tailgate cylinder locks, as well as many glove compartment locks, can be opened in a much easier way. Examine the lock to see if this method is possible. A simple lock that is possible to open in this way is designed to be secured with a retainer accessible from the front of the lock. This lock can be opened by inserting a special L-shaped tool, in effect a 5- to 6-millimeter hook in the end of a piece of stiff wire, through the keyway (fig. 58). The retainer can then be pulled down and worked free. Then the entire plug can be pulled out of the lock and removed. To do this, force the retainer (usually installed with its open ends toward the passenger door) toward the center of the car to disengage it. When the plug has been extracted, the catch mechanism can be pushed back and released with the help of any pointed tool.

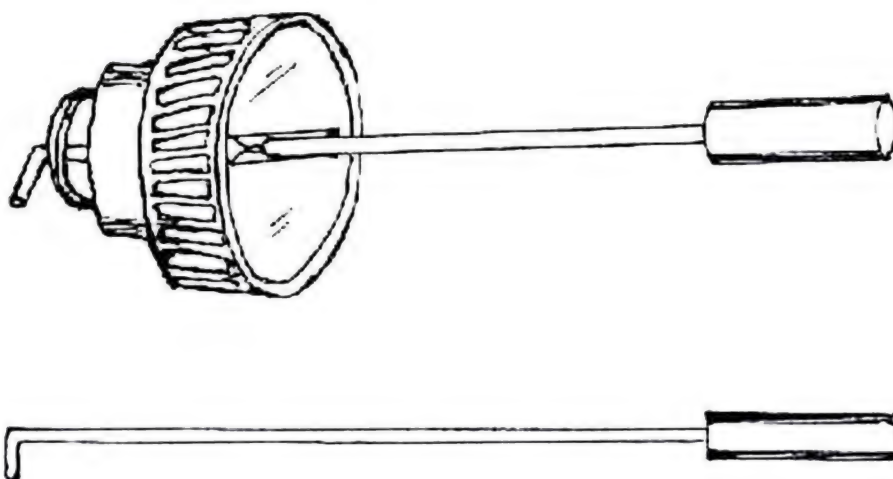


Figure 58. Removing the cylinder from the outside with the L-shaped tool.

There are, in fact, two different locks that can be opened with such an L-shaped wire. The lock in which the plug can be removed has already been described. The other lock is of an even simpler construction. By inserting the wire into the keyway, you can engage the catch mechanism itself and open it by merely pushing it downward.

Methods of Forced Entry

During a forced entry, the actual lock is usually not the target of the intruder. The other components of the lock set and the door (i.e., the striking plate, the hinges, the door frame, and the panels in the door) are generally much weaker. Even the wall next to the door might be weaker and thus more vulnerable than the door itself. The same might apply for the roof or ceiling, or even the floor.

In most buildings built in a warm climate, the walls lack insulating materials. The wall very often consists only of an empty shell, extremely easy to break through with heavy-duty tools. Floors and ceilings are notoriously weak in most countries, whether the climate is warm or cold.

All of these facts help to facilitate a forced entry. The level of force employed in the operation can vary considerably, depending on the circumstances. Sometimes, a low degree of force turns out to be enough. In a few cases, however, the door or the wall area around the main door are smashed through by ramming the building with a car or a heavy truck. A tractor might be used for the same purpose. These are very efficient and quick, if somewhat noisy, approaches to forced entry. Less violence might be sufficient, but in every forced entry operation, it is important to choose the most expeditious method.

DOORS

The door is often the weak link in the protection of the building. The simple fact that the door has to be opened frequently ensures that it cannot be made completely safe. It is important to determine which is the weakest part of the door. If the door is massive, then the lock will be the weakest part, but in fact it is much more common that the door itself is of a weaker construction than the lock installed in it.

If a lock is installed in the wrong way, however, or simply installed carelessly, it may be easier to break through the locking mechanism. Watch for major gaps between the door and its frame. If one of these gaps is large enough, it might be possible to simply insert some suitable object or prying tool through it and wrench the door open.

A cylinder lock is incorrectly installed if the cylinder protrudes more than 2 millimeters. If this is so, then the lock can be forced open by either pulling out the cylinder with heavy-duty tongs or drilling through the now exposed weaker side of the cylinder in order to destroy the locking mechanism.

A lock can almost always be drilled open. In a very few cases, the lock can then be replaced without the owner noticing, at least if it is a cylinder lock. If only the cylinder plug is drilled, the cylinder itself can be saved. Only the inner core needs then to be replaced. However, it is not possible to reconstruct the key afterward. The core has to be a new one, although the external appearance will be the same. When a cylinder lock is drilled open, the lower sets of pins just below the shear line are destroyed, which allows the plug to be turned, as the upper pins can be kept above the shear line with a wire inserted into the lock. There are also various other ways of drilling open a lock, but these will all destroy parts of the lock set that are exposed and clearly visible. The intrusion is therefore obvious and extremely conspicuous. If force of this kind has to be used, then it is better to plan a regular forced entry and simply wreck the entire door.

The area *around* the lock is also a good choice for breaking open. If, for instance, two mortise locks are installed in the same door, the locks should be at least 40 centimeters apart or the door structure will be weakened significantly. Even though the locks might be strong, the door is then easy to break.

In other cases, the screws attaching the lock to the door might be visible, and they might even be possible to remove from the outside. This is another major construction error that makes it easy to force the door open.

Some doors have been reinforced with steel plates fitted on the most exposed parts. If these plates are thick enough and the frame is not significantly weaker, they will cause problems during a forced entry. A carborundum wheel might be necessary to cut through the steel.

Doors with rebated wooden panels and most other types of panelled doors are very weak and can easily be broken with a hefty kick or a hacksaw blade. Aim for the panel next to the lock so that you can reach in with your hand and unlock the door. Be aware, however, that some of these doors have been reinforced by steel sheeting on the inside rather than on the outside. If this is the case, the door might have to be treated as a steel door, despite its inviting exterior appearance.

Some front doors do, in fact, have very flimsy lower panels. They are not only easy to break in through, but they can also be used to push larger objects out of the building. This is a technique often employed by burglars. However, when you are attacking one of these doors, make certain that the panels have not been reinforced on the inside by stronger and thicker wood panels. Such reinforcements can sometimes be detected by the appearance of a number of screws. Wood reinforcements, unlike steel reinforcements, are possible to break through with ordinary tools, but the job will take time and create noise.

Patio doors and sliding doors, especially those with either wooden or aluminum frames, are usually very easy to break through by simply lifting the doors out of the fitting. A patio door lock is a security device designed to bolt

the sliding door to its frame. It is never very strong, though. Some patio doors are even made of plastic today.

Glazed doors are extremely vulnerable. It is not necessary to break a big hole, however. A small hole, sufficient to allow the operative to reach in and open the lock, is quite sufficient. A small area of glass is broken more easily—and safely—than larger ones. A French door, for instance, is likely to open outward, and the latch can be reached and opened easily by breaking one of the small panes of glass in the door. Such a small pane can be broken quietly, without the risk of the neighbors hearing it.

Most doors with a mail slot are very vulnerable to an attack through this opening. Simply put a crowbar through the mail slot and break open the part of the door below the mail slot. This job takes only a few seconds. The latch can sometimes also be reached through the mail slot itself. Special equipment can be made for this purpose.

No door is stronger than its frame. A softwood frame is easily broken. Exposed hinge pins can also be worked upon to open the door. If a wedge was not fitted between the frame and the wall opposite the lock when the house was constructed, then the frame will be weakened significantly. In this case, the frame can often be simply spread away from the door, thus allowing the door to be opened without bothering with the lock mechanism. This is even true of most steel frames, at least those not thicker than 2 millimeters.

Most outward-opening doors can be opened by knocking out the hinge pins and then prying the door open on the hinge side. Alternatively, if the pins cannot be knocked out, the hinges can be sawed off. Therefore, a strong door

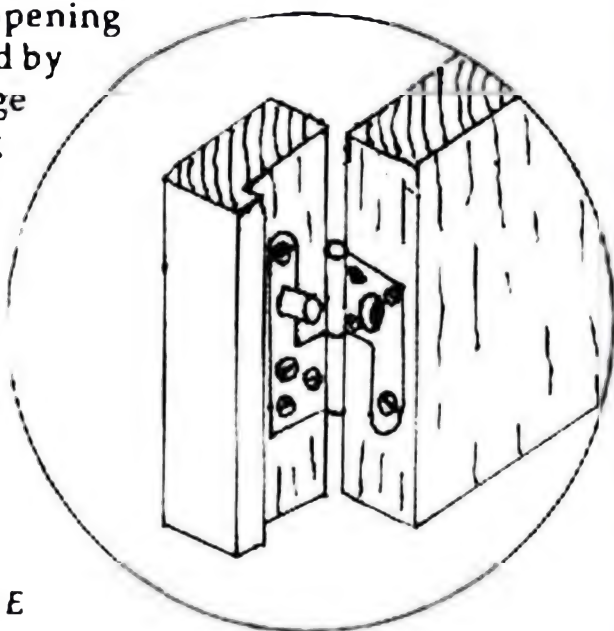
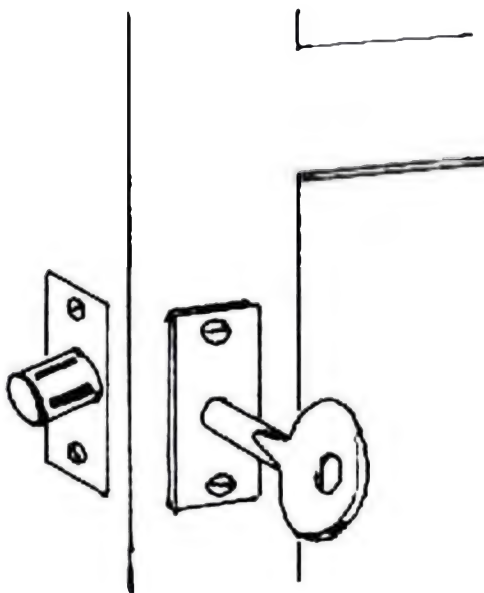


Figure 59. Hinge bolt.

may also be protected by a hinge bolt (fig. 59) fitted in the hinge edge of the door close to the hinge positions. These are studs set into the hinge edge of the door which engage into corresponding sockets, or recesses, in the frame whenever the door is closed. The door cannot then be forced open or lifted simply by sawing off the exposed hinges. Such a door can only be forced by removing either the lock or the frame area around the hinges and the hinge bolts. Hinge bolts are always installed in pairs, one usually below the top hinge and the other above the bottom hinge. Mortise rack bolts are sometimes used for a similar purpose, as for external doors. Such bolts are fitted at the top and bottom of a door and can be locked from the inside with a universal splined key (fig. 60). The lockable bolt is the type most commonly used today. Once again, these bolts can only be locked from the inside. The mortise bolt is a dead bolt, so it cannot be released without a key.

It is worth mentioning that in older houses some doors



and French windows are usually secured with an espagnolette bolt that extends the full length of the door and consists of two vertical sliding bolts, one covering the top half of the door or window and the other covering the bottom half. Both are operated by a central handle, which is often lockable. This works according to roughly the same system and is used to keep the door in place even if the hinges are destroyed.

Figure 60. Mortise rack bolt, locked from the inside.

Barrel bolts are used in many buildings for a similar purpose. These bolts are screwed onto the surface of the door and usually shoot into

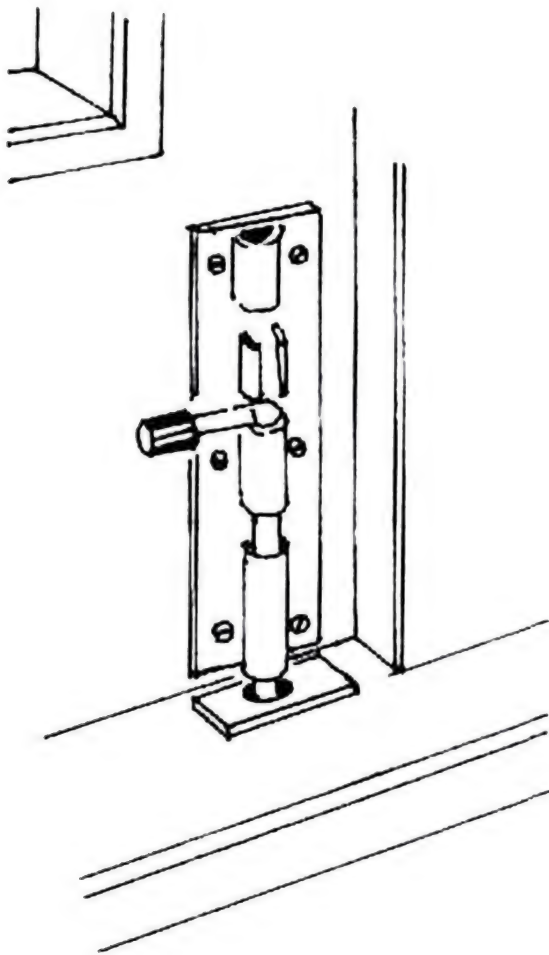


Figure 61. Barrel bolt.

a staple on the door frame. They are usually not fitted with locks. If they are used with a staple, the staple is the weak point, and it can often be forced. If the bolt instead is mounted so that it shoots into the head or sill of the frame, it is much stronger (fig. 61). Sometimes two barrel bolts are used, one for the head and one for the sill. Door chains and door limiters (fig. 62) are devices that pose similar problems for the intruder, but only if somebody is at home and has put the chain or limiter in position.

The limiter is similar to the door chain, but it uses a sliding-rod device instead of a chain. Both these devices are supposed to keep the door safely and effectively closed, even if it has to be slightly opened, such as when receiving a small parcel or a letter. The chain will allow the door to open to about 5 centimeters, but no more.

Certain door chains do in fact have a key-operated lockable staple on the door frame, which allows the occupant to use the chain even when leaving the house. On return, he can open the door sufficiently to unlock the chain from the staple. These door chains can cause a problem for an intruder, unless the staple is weak.

As a matter of fact, many door chains are very weak.

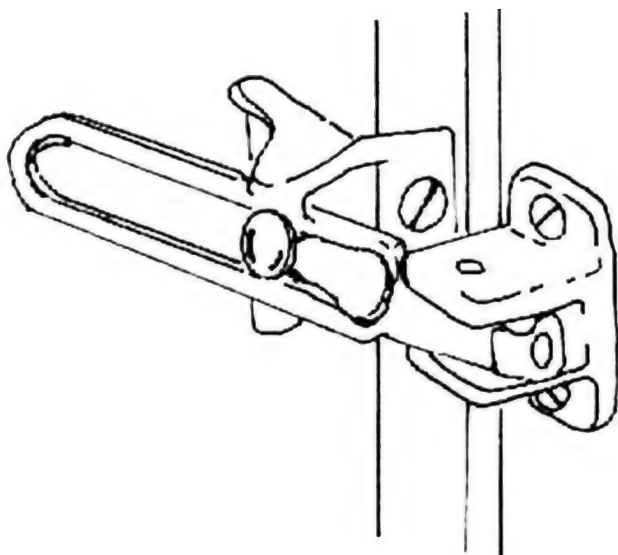


Figure 62. Door limiter.

There have been cases when door chains have been broken as a result of someone merely opening the door without first removing the chain.

Sometimes the door will not be locked properly because of a faulty door check. A door check, or door closer, consists of a heavy spring and arm

coupled to an air or oil cylinder that automatically closes the door. The door check also controls the speed at which the door closes. If the door check is not working properly, there is a good chance that the door remains unlocked.

It is also important to plan the break-in properly. In some buildings, for instance, the front door might be very difficult to break through, but a garage will be attached to the side of the house. Inside the garage there will then be only a lightly protected internal door linking the garage with the home. This door might well turn out to be a much easier target than the front door.

WINDOWS

Windows always present a special problem. There are numerous types of window locks for casement windows, sash windows, and most other types. These locks can generally be picked from the inside, as they are extremely simple and sometimes even all use the same universal splined key. From the outside, however, the only means of entry is to break the window or lock open. Fortunately, the very

construction of a window makes it relatively weak and easy to break. A forced entry through the window is almost always easy. If the window is only closed and not locked, the easiest way to gain entry is to simply smash a small pane to allow one's hand through to release the catch. The window can then be opened.

Window locks will unfortunately prevent the window from being opened in this way. Even if the window is smashed, the frame will remain closed. Climbing through this frame will necessitate noisily breaking a large amount of glass; this is quite dangerous, since the operative is likely to cut himself. Naturally, both these problems should be avoided if at all possible.

In many houses in which the windows are locked, the owner will keep the key to the lock of one window close to the window in case there is a sudden fire. If this key can be recovered or reached, then the window is effectively unlocked. This should be remembered if a window entry is being considered.

Louver windows are notoriously easy to force, especially from a flat roof, such as on a garage, that offers easy access to the window. The louver window can simply be levered out of its frame, unless it is glued very firmly with epoxy resin. In this way, whole strips of glass can be removed from the metal clips. Modern louver windows might have locking devices installed (fig. 63). Sometimes the louver blades are also made of laminated safety glass. Still, a louver window

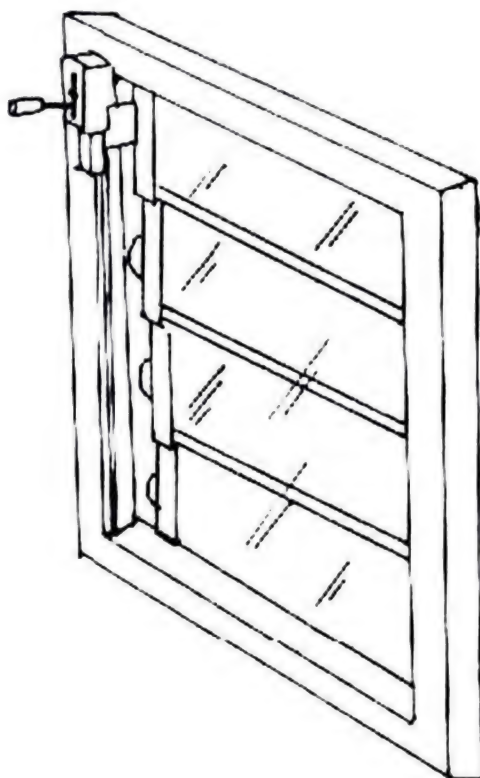


Figure 63. Louver window lock.

will be a good point at which to attempt a forced entry.

Metal window frames in older houses are generally made from steel or galvanized steel and, consequently, are quite difficult to break through. Modern aluminum-framed windows, however, are made of such a thin, soft aluminum alloy that the frames can be distorted easily with a lever of some kind. The self-tapping (self-threading) screws used in these constructions tend to pull out easily, and the locks, if any, are often of a very poor quality. This is especially true of horizontal sliding windows, which work by sliding on an aluminum track. It is often relatively easy to lift such a window out of its track, using the same technique described above for lifting a sliding door.

The important thing to consider when it comes to entering through a window is the type of glass used in the window. There are several different types of glass available. The lowest quality is sheet glass, a cheap glass with imperfections. It is also often referred to as horticultural glass, as it is used for glazing greenhouses. It is generally not used for domestic glazing. A sheet is 3 millimeters in thickness and will break easily.

The standard material for domestic glazing is float glass, which is flat and free from imperfections. It generally comes in thicknesses ranging from 3 to 10 millimeters. Glass that is 4 millimeters thick is very common, but the thickness is always related to the size of the window; a larger window requires thicker glass.

Wired glass is a rolled glass in which a wire mesh is embedded during manufacture. It is 6 millimeters thick and can come both with square or diamond-pattern mesh. If the wired glass is hit by something, the wire will hold the glass together. Its resistance to impact is high, so it is often used where fire-resistance is important, as well as on glazed roofs on which snow and ice are likely to fall. Wired glass is generally not used for security glazing, however, as the mesh can be broken through once the glass has been smashed.

Laminated glass is true safety glass. It cracks but does not break under impact. This glass is formed by two sheets

of float glass with a thin sheet of crystal-clear plastic sandwiched between them. It is very strong. Although the glass will crack under heavy impact, the plastic will hold it together very firmly. This is the most common type of security glass.

Tempered glass, also known as toughened glass or armor-plate glass, is heat-toughened safety glass that is both impact- and fire-resistant. When it does break, it shatters into numerous but harmless pieces with no sharp edges. Tempered glass is four to five times stronger than ordinary glass of the same thickness.

Many other types of glass, such as patterned glass, solar control glass, etc., are also in common use but are not encountered very often during a break-in. They fulfill no special security purpose. Of these various types of glass, only wired, laminated, or tempered glass will resist a sledge hammer, and the wired glass can still be broken through with the help of other tools. Most types of glass can be broken eventually, but doing so is sometimes too time-consuming and noisy to be truly efficient.

The intruder breaking into a window must also look out for venetian blinds. These create two different problems. First of all, it is often very difficult to see through them to determine whether a room is occupied or not. Secondly, breaking through them makes a terrible noise. For these reasons, windows with venetian blinds should be avoided.

SECURITY BARS

Another problem for the intruder will be the existence of security bars. Such bars, used as reinforcement next to an existing door or as a decorative grille for a window, are very difficult to remove, except through brute force or the noisy use of a carborundum wheel. Grilles, especially large sliding grilles (fig. 64), are commonly used in many countries for protecting large areas of glass or doorways. Other grilles are of the detachable type, locked in place with only fixed locks or padlocks. If this is the case, the locks are the weak links in the construction.

Some older buildings rely on solid wooden shutters

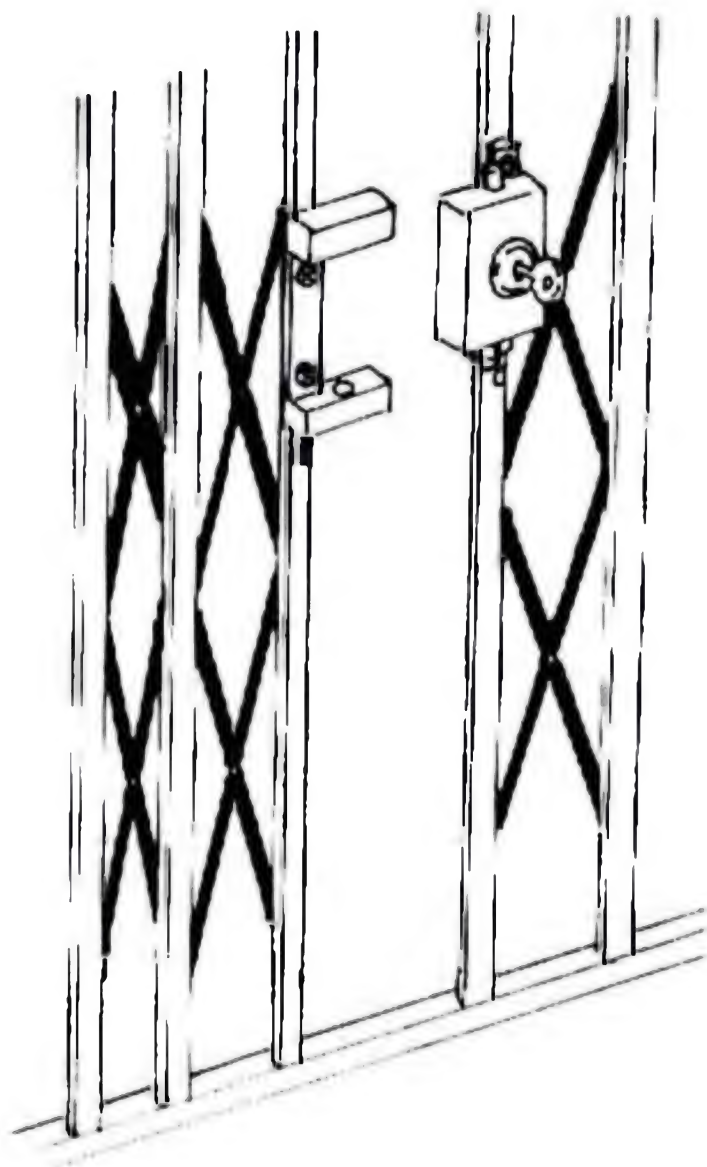


Figure 64. Sliding grille.

instead of steel grilles. Wooden shutters of the louvered type are especially easy to break through, so they present no special problem.

SAFE CRACKING

There are many different types of safes. Some of them are built to be resistant to burglars, while others are resistant to fire. Some are designed to resist both. Most safes can

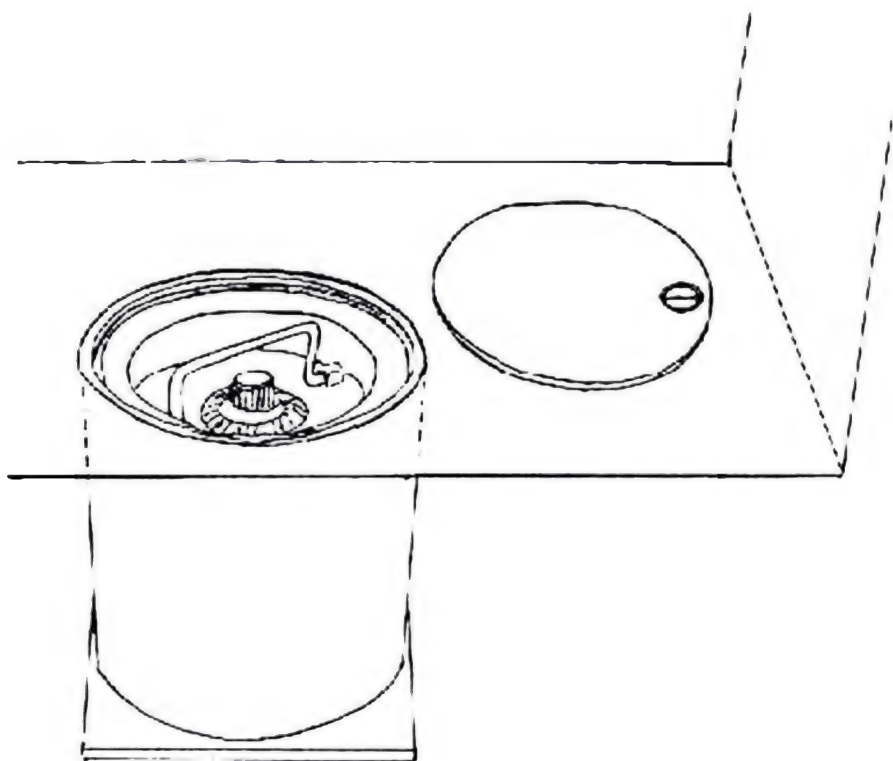


Figure 65. Floor safe.

be cracked without too much trouble, although the contemporary models are more difficult than the older ones. The main problem with cracking a safe is that it creates a large amount of noise. Furthermore, most safes are too heavy to move from their location, so the work must take place on the premises. If the safe is small and light enough and not fixed to the wall or to the floor, then by all means remove it and open it at leisure.

The most reliable safe in a house is the floor safe, as this type of safe is out of sight and can be permanently set in a reinforced concrete floor (fig. 65). A floor safe is recessed into the floor so that the small but strong lid is just below or at the floor level, and it is made of thick steel. Different sizes are available, depending on the depth available under the floor, but the opening will almost always be relatively small.

A safe of this kind is generally positioned in a corner

near the wall, so that it can be covered with the carpet or linoleum and still reached with a minimum of inconvenience. A corner location will also give the intruder less room to work, even if he happens to discover the safe.

A floor safe will not be found in a room where the floor is likely to get wet, such as in a bathroom or a laundry room. Even though it is usually hidden under the carpet, other hiding places should not be disregarded, such as a false floor in the base of a cupboard, for instance. Such a cupboard can be located easily, even in a room with a tiled floor.

A floor safe can also be found fitted in a suspended

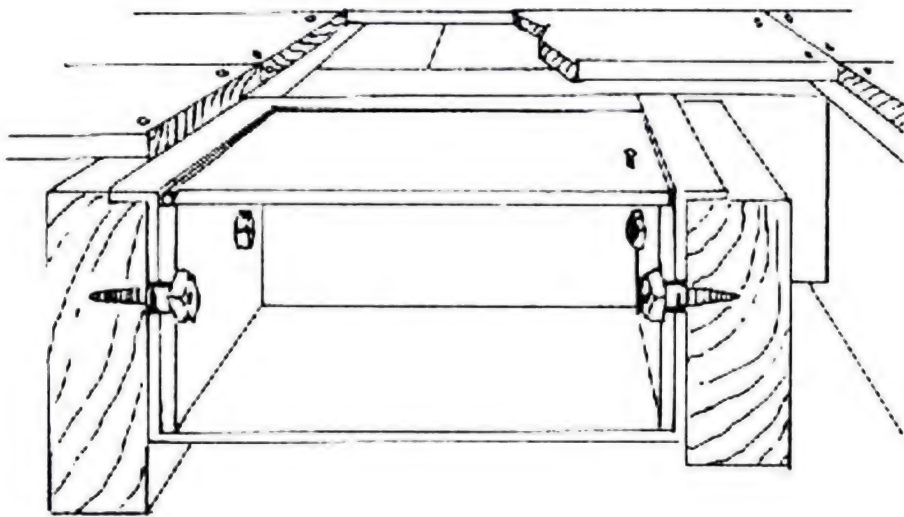


Figure 66. Floor safe in a wood floor.

wood floor (fig. 66). Such safes are in effect secure boxes, often with combination locks, which fit between adjacent joists and are bolted or screwed to them. The screws or bolts are fastened from the inside of the safe. The floorboards will be removable in order to allow access to the safe. The safe itself generally is covered with a sheet of plywood or hardboard to bring the surface level with the surrounding floorboards.

In an apartment complex, the equivalent of the floor safe is the wall safe (fig. 67), which is also easily concealed. A wall safe is a small security box that is set into the wall, replacing one or more existing bricks. The size of the wall safe is mea-

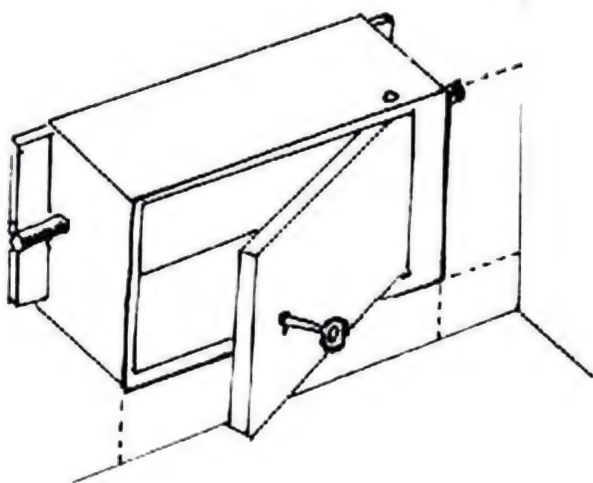


Figure 67. Wall safe.

actually be positioned behind a painting or another picture. Therefore, this is the first place to look for a wall safe. If the

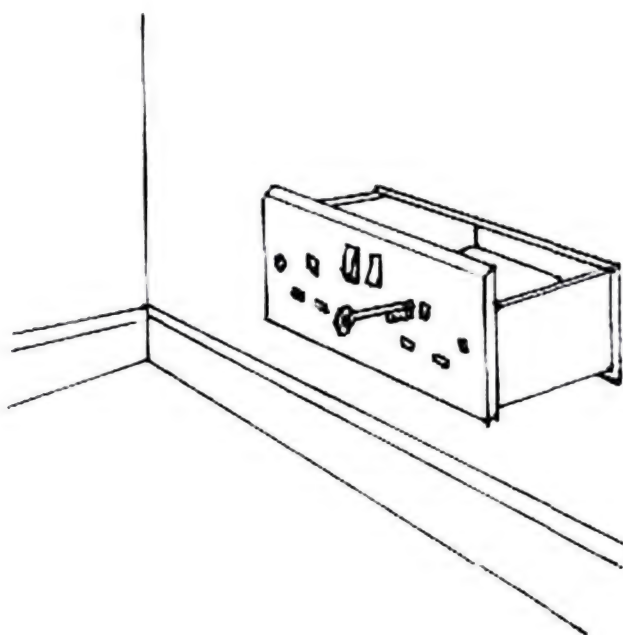


Figure 68. Small wall safe disguised as electrical power socket.

sured by the number of bricks it replaces. Wall safes are therefore commonly one, two, or three bricks high and one brick deep, although double-depth models are also available.

Wall safes are sometimes very cleverly hidden, although it is amazing how often **they** will ac-

tually be positioned behind a painting or another picture. If the wall safe is not in such a place, the owner has been clever, and it could be anywhere. There is even a commercial wall safe the size of a cash box that is disguised to look like an electrical power socket (fig. 68).

A wall safe is easier to breach than a floor safe, as the latter is more difficult to lever out of position. It is also

quite easy to knock out a masonry wall, especially in an older house where the mortar is crumbly. The bricks around the safe can be chopped out with a bolster chisel. The wall safe is then removed and brought to a safe place to be opened.

Certain buildings might have a strong room instead of a safe. These are sometimes difficult to break open, but the principles are the same as with ordinary safes. A strong room is generally less secure than a bank vault, which is very difficult to force open.

The methods suitable for cracking ordinary safes should be helpful for breaking into a bank vault, too. Another interesting point about a bank vault is that it often has a hidden emergency entrance in the form of a hatch. This is to ensure access even if the main door has become impossible to open because of a failed burglary or a mechanical problem. This hatch will of course also be heavily protected, but as it is smaller and usually hidden behind a steel plate, it is not as protected as the main door.

Free-standing safes, especially if not prohibitively heavy, are often secured to the floor, and sometimes to the wall, too. If the safe is not secured in this way, the best option is to simply remove it and crack it open at leisure in some safe spot. All safes are cracked most easily with the help of a carborundum wheel. The disadvantages of this method are that a steady supply of electricity is required and it makes a terrible noise. Fortunately, sufficient power is in fact available in most houses, although it is prudent to bring an extra set of fuses in case the regular ones have been removed in order to prevent this method from being used on the safe.

Many types of safes rely upon combination locks. These can be manipulated to the open position, but it is difficult. The technique is described in Chapter 2. Combination locks can also be opened by drilling, however. The lock cannot be opened completely by simply drilling, but the drilled holes will help the intruder manipulate the wheels of the combination lock.

If this method is resorted to, drill two 3-millimeter holes

in the back of the lock. Then turn the dial and observe what is happening inside the lock through these holes. The gate can be seen through the hole with the help of a flashlight, or a piece of piano wire can be inserted through the hole as a probe. When you have found the gate and aligned it with the hole, you can note the number on the face of the combination dial. Then determine the distance, expressed in divisions on the dial, between the bolt and the gate aligned with the hole. Subtract this distance from your reading. This will give you the combination number for that particular wheel. After obtaining the first number of the combination, reverse the rotation of the dial and repeat the process with the second wheel. The combination of the third and the fourth wheels (if the latter is present) can be determined in the same way.

There are numerous cruder ways of cracking a safe. Explosives, for instance, can be used. Then it is most common to drill a hole above the dial and insert a finger of a glove or a small plastic bag with explosives. An explosion here will destroy the lock mechanism. However, it is by no means guaranteed that the door will open because of this, as it is fairly common for the door to jam during the explosion. This method is therefore not completely reliable.

Another method, almost as old, is to use nitroglycerine. First drive a steel wedge into the top seam of the door. This allows the nitroglycerine to seep around the inner edge of the door so that the door will be blown off the safe when the nitroglycerine is detonated.

None of the methods requiring explosives are really recommended, as they are both dangerous and create too much alarming noise. A neighbor might be disturbed by the sound of a carborundum wheel, but this alone will not be sufficient to make him or her call the police. After all, many repairmen use this tool. An explosion, however, is quite a different matter.

Another way of cracking older, inferior types of safes is to drill a hole in the corner of the front plate of the door. This plate can then be torn away with the help of a long crowbar in order to expose the lock mechanism. The lock

mechanism can then be manipulated open easily. This method is completely ineffective against modern safes, however, as their doors are massive.

In fact, most of the older methods are obsolete, as the safe doors are laminated with hard steel and beryllium-copper plates. Drilling, for instance, becomes almost impossible. One method that still works is generally known as a "torch job," in which an oxyacetylene torch is used to cut through the safe. This requires bulky equipment and special training. It is not really common nowadays, as a carborundum wheel will do the same job in an easier and safer way.

Most older types of safes relied on fairly thin metal walls, padded by an insulating material. However, after several years have passed, the insulating material will have compressed, eventually leaving the upper parts of the walls completely empty and therefore very easy to break through.

Another curiosity should be mentioned here. Some companies now market what they call a bionic safe. This is a safe with an integral alarm system, as well as a few other protection devices. The sensor is usually an inertia sensor that will activate a siren and at the same time, through an automatic dialer connected to the nearest telephone, dial a programmed telephone number. If the safe is broken despite these precautions, a self-contained explosion will destroy all materials inside. (It is designed to cause no harm to any people or property in the vicinity, however.) Furthermore, if the safe is opened without authorization, a sudden burst of high-powered light will be emitted. This is to disable the intruder by stunning and blinding him temporarily. This type of safe is not yet in widespread use.

As a final note, it should be remembered that many safes are designed with an outer construction that imitates high-quality wood paneling. This is both to hide the safe and to make it fit inconspicuously into a home or office. The best protection has always been to hide the safe well. Therefore, when searching a home or an office, be careful to check all possible hiding places, however small, for a safe.

Alarm Systems, Sensors, and How to Avoid Them

According to data from the British police, as many as 98.6 percent of all alarm calls are false. Similar data can be found in most other countries. Clearly, a single-alarm call may not be such a great threat to an entry operation. However, alarm calls must be avoided at all costs—especially multiple calls from the same system.

The basic intrusion alarm system consists of:

- a control unit, generally installed within easy reach of the main means of exit and entry, usually the front door. This is the brain of the alarm system
- one or more warning devices, such as sounder boxes containing warning bells or sirens, and/or strobe lights, often fixed to the wall on the outside of the house
- one or more detection devices, or sensors

Other major components include devices for arming and disarming the alarm system, automated dialing equipment, power supply such as batteries, and wiring between the various components.

The control unit is housed in a protective box, generally made of metal, and is situated in a central location in the area to be protected. An indoor closet might be used for this purpose.

Warning devices of these types are sometimes referred to as alarms or annunciators, although the word alarm is most often used for audible warning devices. Additional devices may be fixed inside the house, mainly as a psychological disturbance to the intruder, and so-called silent alarms are also a possibility. In the latter case, a remote signaling system will be used.

The sensor is the device that relays information to the control unit. If the control unit is the equivalent of the human brain, then the sensors are similar to the senses of the human body. A sensor, or detector, is a scanning and screening device. Its effective range is called the detection zone. The sensors are of different kinds and are commonly divided into three lines of defense. The sensors are connected to the control unit, which, after receiving a warning from a sensor, transmits the alarm to the warning device, which will sound the alarm. The various types of sensors will be detailed in Chapter 7.

There are three lines of defense, but in fact four different kinds of alarm protection:

- external alarms
- perimeter alarms
- trap alarms
- deliberately operated alarms

External alarms aim to detect an intruder as early as possible before he actually reaches the main building. It relies on sensors located in the grounds or on the boundary wall or fence. As these sensors are often susceptible to false alarms, they will generally be monitored by a private security staff and are therefore only to be expected in extremely rich neighborhoods or corporate or government installations.

Photoelectric cells are frequently used for this purpose. They can be positioned to protect the entire perimeter. Other common sensors are the microwave fence and the field effect detectors. Special barrier or fence detectors are also used in certain high-risk installations. Another device used for external alarms is the geophone.

Perimeter alarms are designed to protect the shell of the building (i.e., the walls, doors, and windows). The perimeter sensors will detect the intruder as soon as he breaks into the building. Perimeter alarms are very common and are often used in conjunction with trap alarms.

There are numerous types of perimeter alarm sensors. Magnetic reed contacts, photoelectric cells, glass breakage detectors, video detectors, vibration detectors, inertia sensors, infrasound sensors, field effect sensors, plunger switches, and pressure mats are commonly used sensors in the perimeter alarm. Window foil or prefabricated window foil and wire contacts are also used in some older systems.

Trap alarms are detection devices installed at strategic locations within the house to detect an intruder after he has already entered the building. They are also commonly used to protect individual items of great value or importance.

Detectors used as trap alarms commonly include passive infrared detectors, microwave movement detectors, ultrasonic movement detectors, photoelectric cells, magnetic reed switches, pressure mats, light detectors, and video detectors. Other sensors, such as field effect sensors, sound detectors, and heat detectors (not to be confused with the infrared detectors) also fall within this category. Ionization detectors, when they come into general use, will also belong to this group.

Trap alarms also include special alarms used for guarding specific objects, such as valuable paintings, computers, and so on. These alarms can be of many types, but it is common to run normally closed circuits (this will be explained below) incorporated into the main cable to the electronic device, or affix them somehow to the object of concern. When the wiring is cut or pulled from the wall socket, whether or not the power is on, the alarm will sound.

Finally, deliberately operated alarms are also known as panic buttons. They are found in banks, for instance, but also in many private homes. Such buttons can frequently be found in the bedroom and just inside the front door. Deliberately operated alarm systems will be described in Chapter 8.

Basically, there are two main types of alarm system installations. Most systems consist of separate parts, but nowadays an increasing number of systems are self-contained. A self-contained alarm system contains the control unit, the sensor, and the warning device in the same, easily installed unit. Connections on the back of the unit allow the attachment of separate sensors and external warning devices. The self-contained systems have advantages and disadvantages. This is also true of the separate-components systems, however, so it is prudent to plan well ahead when installing an alarm system.

The separate-components systems are highly adaptable and expandable and can therefore be used in any size or type of building. Additional components can also be installed at a later time. The self-contained systems are more easily installed, however. Generally, they are of the tabletop variety and need only be positioned in a room and plugged in to be ready to use. Self-contained systems are also easy to move, both from different rooms in the same building and from one building to another. For these reasons, self-contained systems are more commonly used by people who rent their homes or offices, while homeowners and large companies generally use separate-components systems.

However, there is another, more significant difference between these two types of systems. The sensors used with most separate-components systems are usually designed as perimeter defense (i.e., to detect intruders and sound the alarm before they manage to enter the premises). Older systems thus require an externally mounted key switch, which serves as a remote arming and disarming device. The self-contained alarm systems, on the other hand, are generally designed to detect an intruder after he has already entered the building. Instead of an externally mounted switch, the system incorporates a time delay, which allows a certain time, often fifteen to thirty seconds, to enter the building and turn off the alarm. The alarm will be sounded only if the system is not turned off in time. It must be remembered, however, that self-contained alarm systems can also be connected to perimeter alarm components. If this option is

used, the self-contained alarm functions as a hybrid control unit, relying on both its own sensor and one or more external ones.

In fact, many self-contained alarm systems can also be used in conjunction with separate-components alarm systems without linking them into the same circuits. The self-contained systems are then used in those areas where it is difficult or impossible to place sensors linked by wire to the control unit in the main system.

Otherwise, self-contained systems are used most commonly in apartments, especially those in which the owner prohibits the tenants from installing permanent alarm systems.

Self-contained alarm systems include:

- passive infrared motion detector units
- ultrasonic motion detector systems
- microwave motion detector systems
- self-contained window or door alarms
- infrasound detectors

Self-contained fire alarms are very common in many different types of buildings. All other types of sensors can generally be found only in separate-components alarm systems.

Most large alarm systems consisting of more than one sensor are designed to be split up into zones, whereby different areas of the building are controlled by different circuits. The main advantage of this is that the occupants of the building can choose to activate all, some, or none of the different parts of the system at any given time. For instance, a bedroom can be excluded so that the occupant can move around there without setting the alarm already activated in the hall near the front door.

Each circuit is made up of a series of contacts, all located within the same zone. The alarm will be triggered when any of these contacts is broken. It is common for several different types of sensors to be installed on each of these circuits.

However, all types of sensors, when they are designed to be connected to a control unit, operate as simple switch-

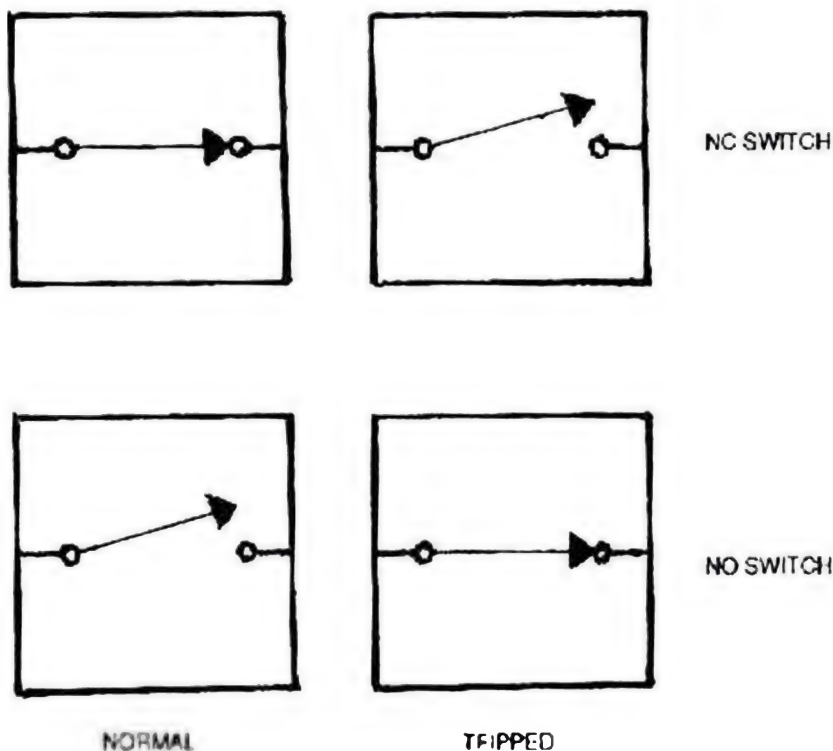


Figure 69. The difference between NO and NC switches.

es. The sensor switch will be either normally open or normally closed (fig. 69). A normally closed (NC) switch is a switch, magnetic or mechanical, in which the contacts are closed (electrically conductive) when no external forces act upon the switch. A normally open (NO) switch, on the other hand, is one in which the contacts are open or separated (electrically nonconductive) when no external forces act upon it. The control unit will sense when the status of one of its sensors is changing and then sound the alarm.

Therefore, a closed-circuit system is one in which the switches and sensors are connected in series. The alarm is sounded when an activated switch or sensor breaks the circuit or the connecting wire is cut. An open-circuit system, on the other hand, is one in which the switches are connected in parallel. The alarm is sounded when an activated switch closes the circuit, permitting current to flow through it. Open-circuit systems are not as secure as closed-circuit systems.

The alarm system must also contain some means for arming and disarming the system. Arming is the means by which an alarm system is switched on. It may be either manual, passive, or remote control. Disarming (i.e., switching off the system) is generally done in the same way.

Some self-contained systems are armed and disarmed by a key switch, while a smaller number are armed and disarmed through a code entered from a keyboard.

A passively armed system will arm and disarm itself when, for instance, the correct key is used for locking and unlocking the front door. This will be further described later in this chapter.

Many alarm systems, however, feature a delayed exit/entrance circuit that permits the user to leave and enter the premises without setting off the alarm. The time lapse is fixed, generally between twenty seconds and two minutes, and can usually be adjusted by the user.

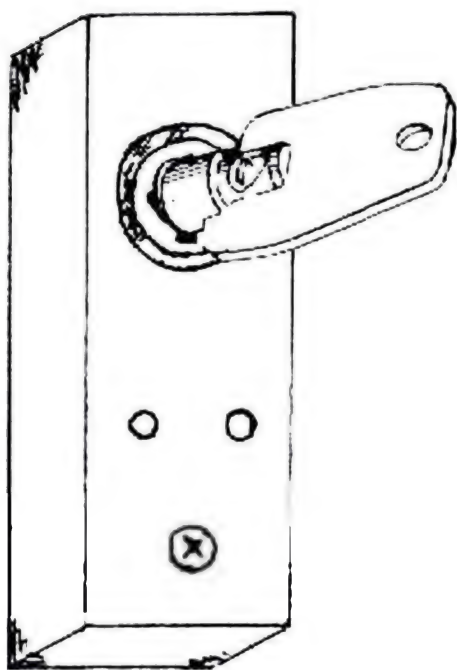


Figure 70. Key switch.

Another common option, especially in simpler alarm systems, is to arm and disarm the system with the help of a key switch (fig. 70). This seems to be especially true of alarm systems in ordinary American houses. The switch is mounted outside the house, and the alarm system will then not have a built-in delay. The lock used in such a system is difficult, but not impossible, to pick. It is generally a tubular cylinder lock. Furthermore, the interior of the lock panel has a tamper switch to prevent

somebody from defeating the alarm. If the switch is damaged, the alarm will sound.

The tamper switch terminals can also be used as a panic button. A panic button is any switch connected to an instantaneously triggered loop. Panic buttons can generally be used whether the alarm is armed or not.

The tamper switch inside the control panel cover is not the alarm system's only protection against sabotage. A self-actuating warning device has an internal battery inside the sounder box. This will take over as power for the siren if an intruder cuts the wire. Tamper protection similar to that mentioned above will often be employed within the sounder box as well.

Other common features used to prevent a skilled intruder from disarming the alarm include contacts which are not easily visible on the surface of door or window frames, hidden components of the alarm system, and the use of four-core cable in the wiring. This cable will allow both closed-circuit devices, such as magnetic contacts, and open-circuit devices, such as pressure mats, to be connected within the same cable. With the former, the alarm will sound if the cable is cut but not if the cable is bridged. With open-circuit devices, cutting the connecting wires will not trigger the alarm, but bridging the circuit will. One pair of wires is used to form the closed circuit, while the other pair is used for the open circuit. The alarm will be set off by one or the other of the alarms if the cable is interfered with.

Even if one of these two types of sensors is not connected, many systems allow the other circuit to run into the sensor and then back to the control unit. This will protect the system in exactly the same way. It will be effectively impossible to sabotage the sensor.

Four-core cable, for the same reason, is also often used together with more advanced warning devices. If the warning device has an integral battery backup, it will then operate even if tampered with or if the wires connecting it to the control unit are cut.

Another option is known as line supervision. This is electronic protection of an alarm line accomplished by sending a continuous or coded signal through a circuit. A change in the circuit characteristics, such as a change in

impedance due to the circuit having been tampered with, will be detected and initiate an alarm if the change exceeds a certain level. A normally closed loop is, in effect, a supervised line.

CONTROL UNITS

The control unit is the brain of the alarm system and fulfills several purposes. It is used to turn the alarm on and off, and it checks the circuits for faults. The control unit monitors the condition of all sensors and sounds the alarm by transmitting a signal to the warning devices whenever it detects a problem. The warning device will also be activated by the control unit if a sensor signals the unit. Of course, the control unit will only fulfill these duties when it is turned on.

The control unit, and in its extension the entire alarm system, functions in the following way. The control unit is connected to the alarm switches, which are connected in a loop circuit. The control unit includes circuits for checking the change of status in these switches, thus detecting when a switch opens or closes (depending on the type). This change will activate the alarm circuit. When the control unit has been activated by a switch, the alarm system is said to be tripped. This activates and sounds the alarm.

Loops of alarm switches are connected to the input terminals of the control unit. There are generally separate terminals for connecting a number of switches, or loops, to the control unit. Each terminal will identify a different loop of switches in the system. Remember that there will be a separate loop for every easily defined area in the building protected by the system. One loop might protect the front door, for instance, while another protects all windows, and so on. In this case, the front door loop will probably have a built-in delay, as this is the entrance to the house, and the owner must have some time to disarm the alarm system. The other loops of the perimeter defense will trigger instantaneously, as these areas are only used for entering and exiting the house by an intruder.

There might also be what is generally known as a day loop. This will also trigger instantaneously, but it will usually only activate a small buzzer instead of the main warning devices. The day loop is sometimes used by families with young children and warns if the children leave through the front or back door or open the gate leading to a swimming pool. This is not really a part of the intruder alarm system, although it uses the same circuits to a certain extent.

The alarm system is said to be armed, or set, whenever the control unit is in operation. Otherwise the alarm system is disarmed. Although control units with more complex circuitry also exist, this is the basic configuration of a control unit. Other features do not much affect the basic functioning of the alarm system. For instance, a system might turn off the warning device when the alarm has sounded for a certain period of time, often five minutes, and then reset the system. Other control units will assign priorities when signals are received from more than one loop in the sensor system. The loop used for fire or smoke detectors will generally override all other loops, for instance. Incidentally, this can be turned to the advantage of the intruder if the protected area is large enough. If a fire is started in one part of the complex during a break-in, the alarm might be effectively hindered from sounding in other parts of the building.

As this description demonstrates, a complex system will include several sensor loops. So the really critical connection is not between the control unit and the sensor loops, but between the control unit and the warning devices. If that line is cut, no warning will be sounded. The intruder should therefore attempt to break this connection rather than futilely trying to avoid the sensors, which is often almost impossible to do if the alarm system is designed properly.

The typical control unit will have both instant and delayed loops. An instant loop will sound the alarm immediately when a switch is tripped, while a delayed loop will wait for a certain period. The entire system will usually have a delay function, at least in modern systems. This

allows sufficient time to arm the system on the way out and disarm it on the way in, and it obliterates the need for an external switch.

Most control units allow the different loops to be turned on or off separately. This is useful for guarding the entrance at night, even if the owner is sleeping in his bedroom, and for allowing the fire alarm to function at all times.

The number of sensors connected to one loop is not limited, even though there is only one set of terminals per loop. The switches are merely wired in series or in parallel (fig. 71). Normally closed switches are wired in series. When the switch opens, signifying that a window or a door is open, this breaks the NC actuating circuit in the control unit and the alarm sounds.

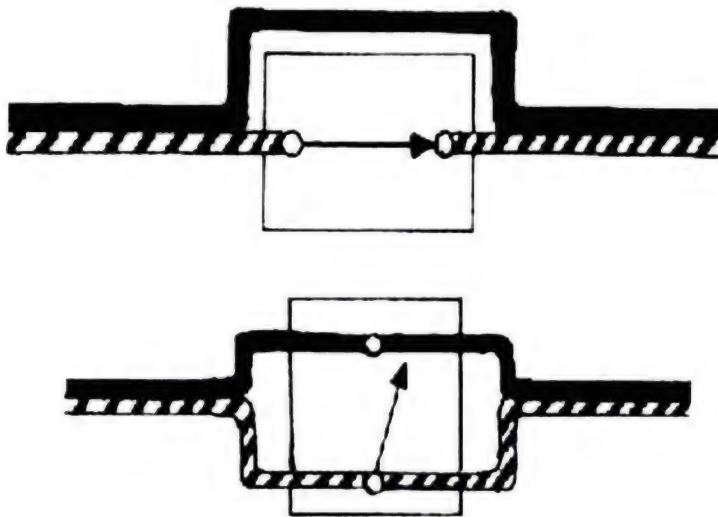


Figure 71. Wiring switches in series (top) and parallel (bottom).

Normally open switches, on the other hand, are wired in parallel. When any of the switches closes, signifying that an intruder has been detected, this completes the NO actuating circuit in the control unit and the alarm sounds. A normally closed switch can be bypassed by bridging the circuit. A normally open switch can be bypassed by cutting the circuit.

A loop of NC switches is generally more efficient, as it is being monitored continuously by the control unit. Any interruption of the NC loop will cause the control unit to

sound the alarm. This is useful if the wiring connecting the switches is broken by an intruder, for instance. The NO loop can be cut easily, and then the control unit will not notice the difference. Remember, though, that a loop of NC switches is often run together with the NO loop in order to serve as a sabotage alarm.

In addition to this sabotage alarm, most professional control units include a plunger switch, known as a tamper switch. This will detect when the door of the control unit has been opened. As the tamper switch is on an instant loop, the alarm will sound as soon as an intruder tries to disable the system by damaging or turning off the control unit.

Often the control unit has an additional tamper switch installed in the back. This switch will sound the alarm if the control unit is removed from the wall. These two types of plunger switches are of the NC type.

As the control unit is often located in a cupboard, this door might also be fitted with an additional sensor that helps to guard the control unit, sounding the alarm when the door to the cupboard is opened.

The control unit can most often be found in an accessible but not easily seen place, such as a closet in the living room or hall, a bedroom closet, or in the kitchen pantry. It will most often be located in an accessible place, however, as it must be reached frequently to be armed or disarmed. An accessible location is not required if an exterior switch is used, of course. Instead of an exterior switch, an interior switch can be used, but this switch will most often be located in one of these accessible places, too, or else near the main entrance.

The control unit must always be installed in an insulated place, so there is generally no need to look in the attic, in a garage, or in the basement. A control unit must always be kept at room temperature. It is often firmly attached to the wall and cannot be removed easily without damaging both the wall and the control unit and also triggering the alarm. Sometimes the actual control unit is completely hidden, while the status of the system is shown on a separate control panel instead. This panel,

even if tampered with, cannot control the system. It will only inform of the current status.

Modern alarm systems are often connected to the mortise lock in the front door. The system will be disarmed whenever the door lock is opened by the key. Picking the lock will produce the same result. One interesting way to disable certain control units is to remove the jumper wires between the unused NC connection terminals. This will, in effect, open the switch, and as the control unit senses an open circuit, it will produce an alarm. Such a minor tampering will leave the impression that the alarm system is faulty, and this might well cause it to be turned off until a maintenance man arrives. Of course, he will notice the real problem. This method requires that the operative disabling the system first gain entry to the control unit and then know how to distinguish between the various switches.

WARNING DEVICES

Most alarms encountered will be local alarms (i.e., alarms that, when activated, will either make a loud noise at or near the protected area, flood the site with light, or both). There are also so-called remote alarms that transmit the alarm signal to a remote paging unit or monitoring station. These could be silent and not give any obvious local indication that an alarm has been transmitted. Sometimes a combination of local and remote alarms will be encountered.

Warning devices come in three basic shapes and in numerous types. All of them are suitable for installation in an alarm system, and any number or combination of warning devices can be used together. Most common are low-voltage sirens or bells, but regular Klaxons are also used fairly frequently.

The sirens are designed to emit a distinctive warbling high/low tone that can be heard over a long distance. In some alarm systems, a siren is used to indicate a burglary, while another siren or a mechanical bell, emitting a steady tone, is used to indicate a fire. An ordinary bell is, nowa-

days, seldom used as an intruder warning device. Instead of a bell, a buzzer can be used, but this, too, is a dated warning device, now generally used only indoors or in factories.

Today, the electric siren is absolutely the most common warning device used. A number of different types are used, but the piezoelectric siren is characterized by the lowest power requirements and is therefore often recommended. The warning device must usually be connected to a battery in case of power failure, so a low level of power is advantageous.

The siren in an intruder alarm system will invariably be of the rise-fall type, as is used in most European countries as a police siren. The design of the siren will not always be the same, however. Some of them are designed for outdoor use, while others are designed for indoor use only. The difference is not only in the level of protection against the weather that its cover will afford the interior circuits, but also in the noise these sirens will emit.

The aim of the outdoor siren is to be heard for as long a distance as possible, while that of the indoor siren is to cause discomfort to the intruder by emitting a really ear-splitting noise, thus scaring him away. For this reason, sirens emitting low-frequency sound are used outdoors, as they have the longest range, while high-frequency-sound sirens are used indoors. Their loud noise will serve as a very effective psychological deterrent to an intruder. Therefore, if the operative must perform a quick break-in without bothering to disarm the alarm system, it is worthwhile to use ear protection.

Yet another warning device, similar to a siren, is the pneumatic warning device. It relies on compressed air and therefore does not need much power. The compressed air, controlled by an electrical air regulator, will produce a very powerful sound when released. Most types of sirens will produce a sound of at least 100 decibels or more, and sound levels of up to 136 decibels are not uncommon.

Another type of warning device is the so-called silent alarm. This is an automatic telephone dialer that will place an emergency call to the owner, the local authorities, or

someone else, and then play a taped message indicating the problem, whether it is a fire or a break-in. Telephone automatic dialers and other remote signaling systems will be detailed in the next section of this chapter.

Some alarm systems, especially those without a remote key switch, will also use a small prealarm buzzer or piezo sounder, which will sound during the entry delay time to remind the owner to disarm his alarm system before the real alarm is sounded.

Finally, there are strobe lights. This type of warning device is especially useful in a crowded neighborhood, where it might be difficult to pinpoint the origin of a siren. The strobe light, if installed, is often the weak link in an alarm system. Such a light will be connected in parallel with the siren or bell used as a warning device, as it is generally only an auxiliary system designed to scare away the intruder and help pinpoint the source of the warning sound from the siren. As this connects the strobe light electrically to the same contacts on the control unit as the siren, the entire alarm will be rendered useless if an intruder first inconspicuously short-circuits the strobe light. This can be done with water if the strobe light is not sufficiently weatherproof or equipped with a tamper switch.

Of course, the wire can also be cut. For this reason, the wiring will usually be hidden or at least out of reach. Despite this, it is remarkable that so many alarm systems can be disabled by simply cutting the wires to the siren or to another warning device.

The warning device, whether a siren or a strobe light, will often be mounted near the eaves or the roof line of the building, at a position at least 2.7 meters high. It might include a tamper switch and will generally be wired through the attic. Needless to say, a favorite tactic of professional burglars is to first of all break into the unprotected attic to locate and cut the wiring to the siren and then break into the house. Sometimes the warning device is instead mounted on a lumber or a metal pole, such as a television antenna. It is not uncommon to mount it directly on the existing mast of the television antenna. This is especially true of strobe lights.

Many, but not all, warning devices will come with a tamper switch, allowing the alarm to sound even if the siren is tampered with. Of course, this is worthless if no other warning device is present. Always look out for an extra hidden warning device before you disable the main one.

In most countries, the sounder box will turn off automatically within a preset time, usually no longer than twenty minutes, so as not to disturb the neighbors. The system will then reset itself automatically. This might not always be the case with the alarm system in a government installation, however. Even if the noise is turned off, there is often an affixed strobe light that will keep flashing until someone manually resets the alarm.

REMOTE SIGNALING SYSTEMS AND AUTOMATIC DIALERS

Nowadays, many alarm systems are linked to a telephone. By using a separate, exdirectory telephone line used only for outgoing calls, they are designed to raise the alarm in a remote location in case of intrusion. These devices, known alternatively as automated dialing equipment (ADE), automatic dialers, autodialers, or telephone dialers, are available in three slightly different varieties.

The reason for using an exdirectory line is that the alarm cannot then be neutralized by calling the automatic dialer. Placing such a call will effectively block the outgoing call. In some countries, the telephone system allows all incoming calls to be routed to a different number, thus freeing the automatic dialer's line.

The simplest type of automatic dialer is programmed to dial the local police and then play a standard prerecorded message stating that there is an intruder in the house. Of course, the message will also include relevant details, such as the owner's name, the address, and the telephone number. This system, although reliable in theory, is frequently useless, as many police forces no longer have the manpower to monitor the lines. Another drawback is that the automatic dialer will not work if the intruder cuts or temporarily disconnects the telephone lines. Furthermore, the auto-

matic dialer will generally only dial its call once. If nobody answers, then it is bad luck for the owner of the system.

Another version of this system works in the same way, but instead of calling the police it will alert a neighbor or a relative who will then call the police. This system is even worse, as the friend might not be at home, and, even if he is home, the call will take still longer to reach the police. Here, again, a cut line will effectively prevent the system from sounding the alarm.

For these reasons, the digital communicator is more popular. This is a more sophisticated system that is able to dial a central monitoring station, usually the security company's central control station or the main security station in a corporate complex. Here, personnel will be on constant duty to observe annunciators reporting on the condition of the alarm system. The alarm call will consist of a series of coded signals that comes up as text on a computer screen which is monitored twenty-four hours a day by the staff. Upon observing these signals on the screen, a staff member will alert the police immediately and often dispatch a corporate security team to the location as well.

The digital communicator will continue to call until the message gets through. This is determined by the receiving station giving a correct code, which means that the message has been understood. In this case, the digital communicator might be programmed to call several numbers until it receives a confirmation from one of them. Some systems are designed instead to confirm by calling back within a specified time. Generally, this type of system is also designed to register any faults on the telephone line, thus announcing the danger of a cut line. This system, too, relies on using an exdirectory line.

Locations guarded by such systems are generally easy to recognize, as the company that installed them will advertise their presence with posted signs. Systems of this kind are almost always rented as parts of professionally installed alarm systems and are subject to regular maintenance inspections by the security company.

An even more advanced system, marketed in Britain and

in certain other countries, also responds to a fire alarm. It will furthermore indicate exactly which zone or loop the alarm has been triggered in and what type it is. Any faults on either the line or in the alarm system will also be reported.

The most exclusive alarm systems use direct private lines rather than the ordinary telephone lines. In this case, the alarm signal will be transmitted on a continuously monitored private line to the security company's central monitoring station. Any fault or interference with the line will be noticed. Such a system is in use only in high-risk installations or on the premises of the extremely wealthy.

If an ex-directory or a private line has not been used, the automatic dialer must always be connected as the primary telephone in the house. This means that all incoming calls must pass through the automatic dialer and then proceed to the regular telephone. If this is not the case, the system, even if it is hidden, can be easily disabled by removing the regular telephone's handset from the hook.

Some automatic dialers have their own built-in backup batteries, which allow them to work for several hours even if the power is cut. The power will ordinarily come either from the control unit or from a separate AC power adapter.

The recorded message will either be on a magnetic tape, in which case the owner can record his own message, or it will be a prerecorded computerized voice. Most automatic dialers can be programmed with up to three telephone numbers, all of which will be called in order.

An interesting point about some of these systems, especially the British ones, is that some police forces insist that the siren, if one is used in conjunction with the remote signaling device, have a built-in delay so that it will sound the alarm three to five minutes after the message has been relayed to the police. This is to give the police a greater chance of the catching the intruder in the act.

It should also be noted that even if the automatic dialer is connected to a security company, it is by no means certain that they will care to respond to a single indication of a triggered alarm. False alarms are now so common that most companies of this type will wait until they first have received

an alarm from an external detector, then from a perimeter detector, and finally from an interior detector, indicating that this is a serious intrusion attempt. Only then will they dispatch a patrol or call the police. This reluctance to respond to false alarms will give the operative a few valuable minutes in which to execute his mission and get away.

A radio transmitter can also be used as an automated dialing system. In this case, it is most common to use a transmitter in the frequency-range around 27 MHz, as this is most commonly used in personal paging systems. A radio system utilized in this way is most common in advanced alarm systems in vehicles, boats, and other places in which there is no regular telephone connection.

The suitability of the antenna is the most important factor, as this will determine the range of the system. If the antenna is removed, or covered by a metal box, the transmission will suffer a severely decreased range or even disappear completely. Naturally, no remote alarm will then be sounded.

ACCESS AND EXIT CONTROL SYSTEMS

Access control is the means by which only authorized persons are allowed to enter a building or flat while unauthorized persons are kept out. Such a system is commonly designed around an exit-entry control system and /or a system to arm and disarm the alarm system. For these purposes, there will be an authorized access switch that makes all or parts of an alarm system inoperative in order to permit authorized access.

In most doors the mechanical lock is the only access control system. There are, however, a large number of other possibilities, mechanical and electrical, sometimes used only as keyless locking devices, but sometimes also used together with alarm systems. In the latter case, the system will definitely rely on electrical control switches. Most of these control systems require the use of combination codes. See Chapter 2 for more information on this.

Electrically operated locks are becoming more and more popular, especially in industrial installations and offices. So

far, however, electrically actuated release catches are more common than pure electronic locks. These units operate on low voltage, often 24 V. For this reason, they need transformers. Locks that are normally locked will be unlocked when the system is energized. On the other hand, those that are normally unlocked will lock when the unit is energized. The first option is of course most commonly encountered by an operative desiring to enter.

It is sometimes possible to enter by connecting a high power source to the lock, thus overloading the circuit. However, there is also another factor that must be taken into account. Some locks of this type are so called fail-safe. This means that they will automatically unlock if the power fails, such as might happen in an emergency such as a fire. This is to provide a safe escape route, of course, but it can serve equally well for purposes of gaining entry to the premises. In short, tampering with the power supply might well open a lock of this type, as long as you know what type of locking device you are dealing with.

Also note that there might be a considerable distance between the actual lock and the remote control unit. Most commonly, the control unit is next to the door, and it is always built around a control switch. There are many types of control switches. Among them are digital access control systems, electronic or mechanical card access control systems, lock switches, remote control switches, delayed alarms, and ordinary key switches. The various systems may rely on number code combinations, coded cards, or plastic keys instead of metal keys. This is common in hotels and in many hospitals, for instance. As these systems are quite often electronic, they are also frequently connected to a registration unit, able to record when a certain code or key is used and where, if the system includes more than one lock.

The digital access control system is perhaps the most common of these systems. It usually consists of two parts: an access control keyboard and a program unit. Such a system can possibly use ten thousand different code combinations. Every legitimate user might have an individual code,

or everyone might use the same one. The code might be used for opening the lock or for disarming or arming the alarm system.

Less commonly, a dial of the type used in combination locks can also be used in this device. Both types are very popular with large companies, as it might be necessary to change the code from time to time, such as when staff is replaced.

There are digital systems that only close the circuit momentarily, thus turning off the alarm system and/or opening the door for up to ten seconds or so. Others remain closed until the code is reentered. Some systems allow the use of different codes for different individuals. Most of these switches will only disarm one loop, consisting of the sensors that guard the nearest way to the control unit, so that the owner can proceed there immediately to disarm the entire system.

Usually the code will consist of either four or six digits. Occasionally the four-digit code will serve as a code lock, while the six digits will arm or disarm the alarm system. Sometimes the lock will not unlock until the alarm system has been disarmed. It is also common for the code lock to temporarily block another attempt if the code entered is the wrong one. This is to discourage attempts to enter by using random combinations. Some systems go even further, triggering an alarm when a preset number of incorrect combinations has been entered.

Most systems of this type will also have a preset timer that is activated when the first digit of the code combination is entered. If the remainder of the code is not entered before the time expires, the entry is canceled.

Yet another interesting feature of some of these systems is what is known as a duress alarm. This is connected to an alarm system and a warning device, such as a siren. A silent alarm is also a real possibility here. The duress alarm is activated by depressing the correct combination code but replacing the last digit with a predetermined other digit, known as the duress digit. This will or will not open the lock, depending on the programming, but it will definitely trigger the alarm. This is to warn against entry made under

duress, for instance, by an employee who is held at gunpoint by an intruder. Technically, this system is a momentary switch with NO switch contacts.

Another unit, very often used in conjunction with this device, is the card reader. A card-based access control system is easy to use and therefore popular in large corporations and government installations. The card reader is situated next to the door, requiring the person wishing to enter to both insert his coded access card in the reader and punch his personal code on the keyboard.

The plastic cards for these locks are of two different types. They can either rely on a magnetic code, in the same way as a credit card, or they can have various optically read numbers or figures. In either case, the card must be entered into a slot or passed through a card reader situated at the door. There are also systems in which the card reader is invisible, hidden in the wall next to the door, and the card is simply displayed roughly 30 centimeters from the reader in the wall.

Whatever type is used, the card will have a code that allows entry through only one or several doors, depending on the design and programming. All cards can have the same code, or individual codes might be used instead. The system is extremely flexible. A plastic key with a code in it can also be used. This works exactly like the card keys but is designed to be carried like an ordinary key on a key ring.

In certain of these locks, however, the system is not electronic but mechanical, even though the key is still replaced by a plastic card. When a plastic card with holes in it is used, the lock is definitely mechanical. The holes in the card will fit exactly to a number of balls within the lock. The lock can be individually coded, and the code can be changed easily. The card might have a code allowing access through several doors or only one. Note that this is not a real code, but only a means of ensuring that the card fits into its slot in order to open the door. Consequently, it is the same as the cuts on a regular key.

A door protected by a code lock or card lock will often have an alarm sensor as well, which will sound the alarm if

the door remains open too long. Sometimes this will only be a buzzer to indicate that the door must be closed, but occasionally a real warning device will be used.

Electronic locks may also take advantage of time coding. This is a system that is programmed to allow or deny access, depending on the time of the day or night. Every legitimate user might be allowed to enter during ordinary office hours, but only key personnel will be permitted to enter after office hours. When a system of this complexity is used, an automatic registration unit will almost certainly exist. A system of this type can be made very flexible indeed.

If a card is lost, the code (if one is being used) will be changed as soon as the owner becomes aware of the loss. The person who lost the card will simply be issued a new card and a new code. Changing the code is a quick process. The number of possible combinations is very high.

It is difficult to bypass access control systems of this type. The keyboards and card readers might be vulnerable to weather, but this will not allow access; it will only prevent it further. There are, however, a few ways of cheating such a system.

If the same code has been used for a very long time, it is sometimes possible to see which numbers are being used, as wear and tear together with dirt will show which keys are used most commonly. The combination is then not obvious, of course, but the number of possible combinations will decrease significantly. This has often helped the enterprising operative to gain entrance.

Another common way of learning the code, at least in those locations where no card is required, is to simply observe somebody entering from a distance. However, many keyboards have been fitted with protective covers to prevent this from happening.

Electric digital code switches can sometimes be shorted by connecting a high-power cable to them instead of the ordinary low-power cable normally used. This might open the lock, but only if it is of the correct type, the one that will unlock when energized.

In private homes, the access control is usually simpler.

One common access control system is the lock switch. This device fulfills two purposes. The first is to disarm the alarm system, while the second is to unlock the door. The system is usually installed in the mortise lock in the front door (see the section of this chapter on lock switches built into standard, mechanical mortise locks). This is common in private homes, where the number of keys is limited. When this system is used, the door and its frame will often be protected by an inertia sensor, for instance (see the section on vibration detectors and inertia sensors in Chapter 7).

Remote control switches are another possibility. They come in two major types. The most common is the radio transmitter operated switch, but infrared operated switches are also used commonly. This system is often used in garage doors. The remote control will open the door and disarm the alarm system at the same time. Remote control switches, especially of the radio frequency (RF) type, are also common in perimeter alarm systems around outlying sheds and stores. The alarm is then built around the sensors mounted on the surrounding fence, but the remote control device can arm and disarm the control unit, located inside the shed or store. The range will then be around 70 meters, which is usually enough.

The radio transmitter will transmit a digitally coded signal. This signal, when recognized by the receiver switch, will arm or disarm the alarm system, or parts of it, if so desired.

Delayed alarm systems are also common. The alarm will simply be delayed so that the operator has enough time to reach the control unit and turn off the system before the alarm is sounded. The delayed alarm was described in more detail in the first section of this chapter.

It should be pointed out that some corporate alarm systems are not armed and disarmed manually at all. Instead they rely on a timer switch that will turn the alarm system on and off before and after office hours. Note that the time will not necessarily be the same every day of the week.

A key switch, finally, is exactly the same as a standard lock, but it is connected to the alarm system. It is usually in

a small box, protected against sabotage by a tamper switch, and located outside the building. As the switch can sometimes be tampered with by exposing the wires going to the key switch, it is often at least set into hard material and is usually also protected by an inertia sensor.

Electric locks were described previously, but another problem might be electromagnetic locks. These are used in hospitals, banks, prisons, airports, and numerous other high-risk installations. The interesting thing about the electromagnetic lock is that it can exert a very strong holding force. In fact, the lock consists of two components, the lock itself and its armature (fig. 72). The lock is mounted to the door frame, while the armature is mounted to the door. Both mountings are designed to be sturdy and resistant to physical abuse. The lock and the armature will make con-

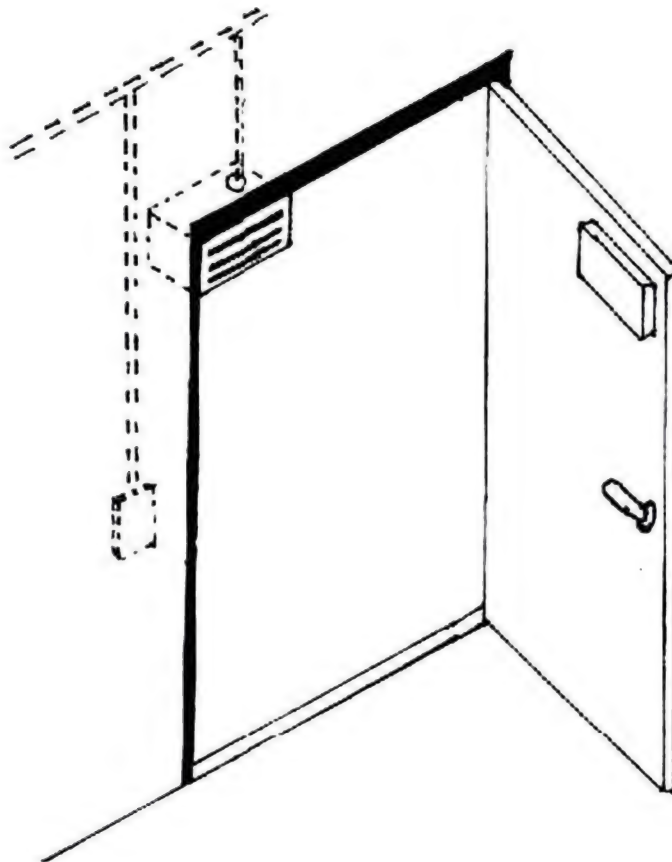


Figure 72. Electromagnetic lock.

tact when the door is closed. Locking, or activating, the lock will cause the two units to be magnetically attracted to each other and hold together. The wiring will be factory-made and includes tamper-resistant circuits. The easiest way to disable the electromagnetic lock is to deprive it of energy. However, this is not always so easy.

LOCK SWITCHES BUILT INTO STANDARD MECHANICAL MORTISE LOCKS

A lock switch can also be built into a standard mechanical mortise lock (fig. 73). The lock switch fulfills two purposes. The first is to disarm the alarm system, while the second is to unlock the door. The standard key to the lock is used, and while the key will unlock the lock, the switch

will disarm the alarm system. The system is usually installed in the mortise lock in the front door, although other secure locks, such as tubular locks, might also be used for this purpose.

This device is common in private homes, where the number of keys is limited. When this system is used, the door and its frame will often be protected by an inertia sensor. It is possible to pick this lock. An even greater danger is the key to the lock, as this will not only allow

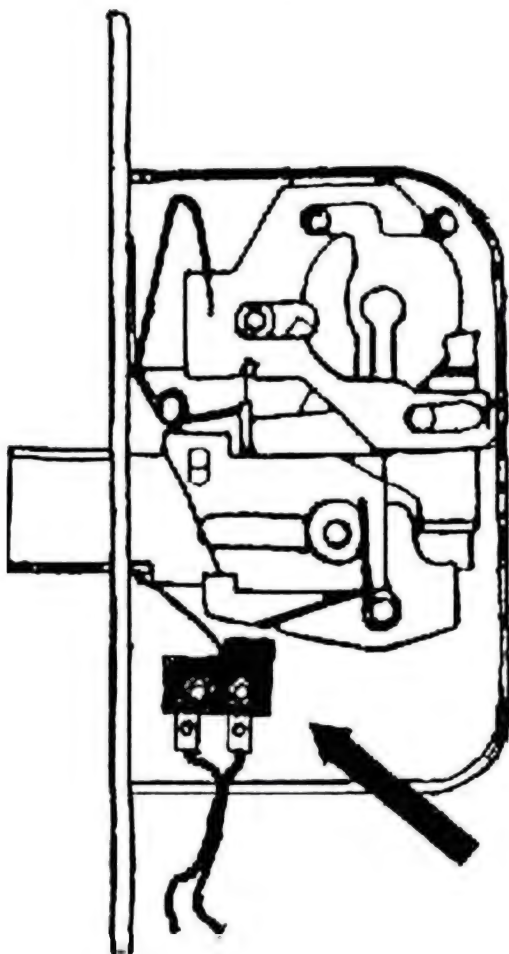


Figure 73. Lock switch installed in mortise lock.

entry to the building but disarm the entire alarm system as well.

The lock switch is a standard contact switch, which is mounted inside the lock next to the latch bolt. The switch will react when the latch bolt is moved to the locked or unlocked position. Such a switch is, in itself, relatively easy to manipulate, so other means of protecting the switch are usually installed.

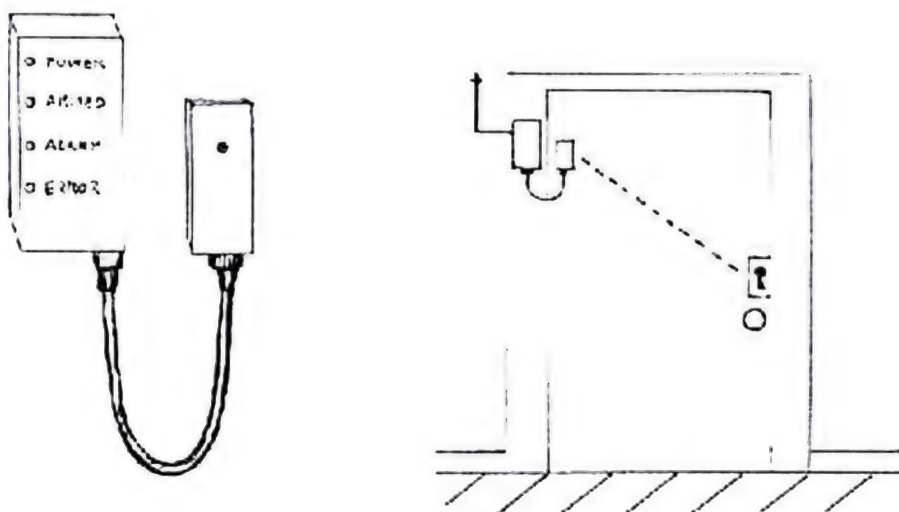


Figure 74. The jumper cable terminal and its position on the door frame.

One efficient protective system is to use a mortise lock along with an inertia sensor built into one of the jumper cable terminals mounted on the door frame (fig. 74). This sensor will protect both the lock and the door. There is also an LED in the face of the lock. This LED will not only indicate that the alarm is armed by flashing, it will also work as a sabotage protection, as its circuit will trigger the alarm if it or the lock is damaged. Furthermore, if the power is not sufficient, the LED will stop flashing and instead remain on continuously. This also happens if the alarm has been triggered. The system will reset automatically every time the door is locked.

The switch circuit is a NO system, open when the lock is locked and closed when the lock is unlocked. The wire is usually of the four-conductor type, however, two of them

being the NO circuit and the other two the NC sabotage defense. The wiring is run either through a diagonal hole in the door or on top of the door. An alarm of this type can also be used if several doors are to be used as main entrances. The locks and their systems will then be connected in parallel. Then the alarm system will be disarmed whenever any of the locks are unlocked. However, the system will be armed only when the last unlocked lock is finally locked.

POWER SUPPLY AND BATTERIES

Most alarm systems are powered through the control unit. Generally, the power supply is housed in a separate transformer box plugged directly into a wall outlet. The transformer converts the AC current to 12 volts DC, which is used for the entire alarm system. The transformer is attached to the control unit by an ordinary two-conductor wire.

If the intruder can legitimately gain entrance to the building to be searched, for instance during office hours, it is sometimes possible to locate the transformer and simply remove it from the wall outlet. As most alarm systems will have a battery backup power source, the alarm system will switch to battery power at once, usually without alerting the inhabitants of the house. This is generally enough to last for several hours, but it will run out soon after the occupants have left the building in the evening or gone to bed at night. Such a method is often helped by the fact that most wall outlets are in low and inconspicuous locations, such as behind furniture. Even though the control box might be checked in the evening, the transformer will most often not be checked.

Backup batteries are commonly used because burglars have learned to shut off the electricity in the house they are going to enter. The backup batteries are rechargeable and are usually installed in the control unit. The rate of discharge depends mainly on whether a siren has been activated or not, as this consumes a large amount of power, but the backup protection will generally last for around three hours—or less if the siren is used.

It should be noted, however, that in many European countries the backup batteries are more often designed to last for at least twenty-four hours or even seventy-two hours (a normal weekend). If the alarm system has no backup batteries, the system will always come back on armed if the AC power has been cut off temporarily.

Some control units will check the status of the batteries each time the system is armed or disarmed. This is to inform the user of the fact that power is low.

As a curiosity, it might be mentioned that certain external control panels, installed to monitor the current status of the alarm system, also monitor the fact that the current required to recharge the backup batteries is insufficient. This is to advise the owner that he must check and possibly repair this function. Opportunist burglars are thankful for this information, as they then know that it is safe to break into the house as long as they cut the power first.

WIRING

Most wiring connecting the various sensors to the control unit will be concealed, or at least located very unobtrusively. The wiring is frequently run inside the interior walls. A small hole will be drilled near the sensor. The wiring will go through this hole into a larger hole in the sole or top plate in the basement or the attic. The wiring will be run there, following the attic or basement until it once again penetrates into and surfaces through a small hole next to the control unit.

Wiring can also be hidden under carpeting, beneath floorboards and masonry trim, or behind furniture. It is generally not placed where it might get damaged by water, excessive moisture, or local pests (rats and other rodents tend to bite through electrical wiring).

It was mentioned above that a loop of NC switches is often run together with the NO loop in a four-strand cable to serve as a sabotage alarm. This is not the only way of protecting the alarm system against sabotage. The most inconspicuous defense is the balanced alarm system. This

is impossible to detect from the outside or even from the inside of the building, as long as the control unit is not found and opened.

A balanced system consists of a number of sensors, just as an ordinary system, but every sensor will be fitted with a unique resistor. The control unit will then be adjusted to recognize the total resistance of the system. If one sensor is shorted or bypassed, the control unit will detect a decrease in the system's total resistance. This will trigger the alarm immediately.

It should also be remembered that some contemporary alarm systems utilize built-in computers to control the system. This means, among other things, that any changes in the system's status will be recorded, even if the alarm has not been sounded.

More advanced alarm systems will employ computerized communication on two or four wires to further protect the system against sabotage. The computer will regularly query the various detectors about their status. The entire net of wiring will be monitored in the same way. As this system is almost always connected to a central alarm, the entire system, including any detected irregularities as well as triggered alarms, can be presented on a computer monitor. One example of this system is the U.S. Vindicator system, installed to protect air bases and important defense industries but now commercially available to major companies as well.

In this case, every detector is connected to a transponder, which will report through time-multiplexing every change in wiring or any indication given by the detector. These reports will be presented in real time to an alarm operator in the security central. The system is therefore extremely difficult to bypass, and here it is definitely easier to try to subvert the human computer operator in the system, as he is the weakest link in the chain.

WIRELESS SYSTEMS

Wireless alarm systems are also used fairly frequently.

They are more expensive, but they are also easier to install than the wired systems. Such an alarm system consists of a central processor unit and one or more detection devices. All these components communicate by using radio waves. The radio frequencies used are supposedly free of interference from any other radio-controlled equipment such as the communication radios in passing taxis and police cars.

The entire alarm system is controlled by a small radio touch-pad, about the size of a pocket calculator. This remote control can be used to activate the alarm from anywhere in the house. It can also be used as a personal attack alarm, or panic button, wherever the user is, whether in the house or outside in an adjacent garden or garage.

In the United States, some wireless alarm systems are available that not only sound the alarm but also regulate the turning on and off of lights and other electric appliances, such as television sets. These devices are supposed to scare away intruders by pretending that somebody is in the house, even when it is in fact empty. This device is either battery-powered, or it takes its power directly from the AC power supply. In the latter case, the entire system will fail if the power is cut. If batteries are being used instead, the battery-powered transmitters will be supervised every ninety minutes or so to determine battery and functional condition. This will safeguard against loss of power, but only as long as the control unit itself remains powered, of course.

Wireless alarm systems must not be mixed up with self-contained alarm systems. The latter also sometimes rely on radio, but work in a different way. A real wireless alarm system is in effect a separate-components system, but using radio waves instead of wiring.

Alarm Sensors

There are many different types of sensors, and they are often categorized broadly as active and passive. Active sensors create a field and detect a disturbance in that field, while passive sensors detect natural radiation or radiation disturbances without themselves emitting the radiation on which the sensor's operation depends.

Sensors are also divided into categories based on the area or particular point that they protect. Perimeter protection prevents access to the outer limits of a protected area by means of physical barriers, sensors on these barriers, or external sensors not associated with any physical barrier. Interior protection is a line of protection along the interior boundary of a protected area, usually a building, including all points through which entry can be made. Area protection, finally, covers an inner space or volume of a secured area by means of a volumetric sensor, or a sensor with a detection zone that extends over a volume, such as an entire room.

MAGNETIC REED SWITCHES AND WIRE CONTACT SYSTEMS

A magnetic reed switch is an alarm system detection device in which a disruption of the magnetic field between two points causes a break in the electrical current. This

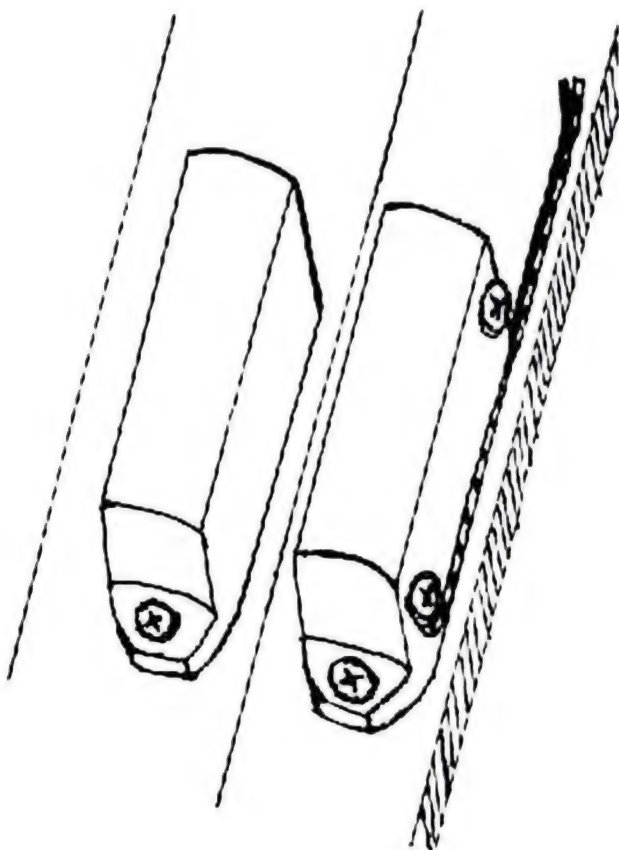


Figure 75. Magnetic reed switch.

break signals the control unit to activate the alarm. Magnetic reed switches (fig. 75) are among the most common alarm sensors in use today.

Magnetic reed switches are a type of magnetic switch that consists of electrical contacts formed by two thin, magnetically actuated, reedlike metal vanes, held in position (normally open or normally closed) within a sealed glass tube. The tube is enclosed in a metal or plastic case. The device works on the principle of magnetic attraction. The sealed metal contacts are positioned in such a way that when a sufficiently strong magnetic field is present, they are either pulled together or pushed apart (fig. 76). When the magnetic field is removed, the metal contacts will naturally move in opposite directions.

The reed switch is therefore composed of two separate units: the magnetically actuated switch and a large magnet, which is enclosed in a similar plastic housing.

The contacts within an NO reed switch do not touch

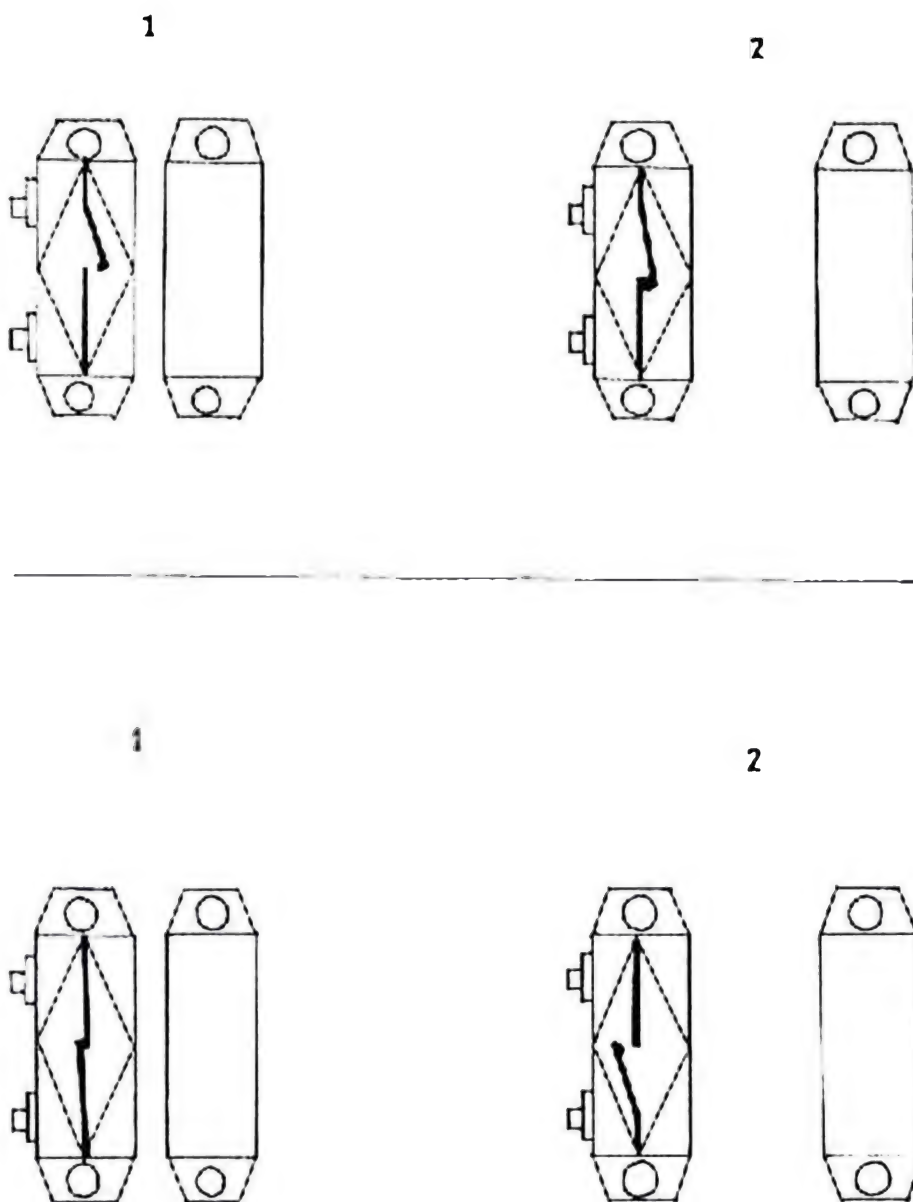


Figure 76. NO and NC magnetic reed switches.

when the magnetic field is strong enough. The loop will be normally open. But when the magnet is removed, the contacts will be pulled together, closing the contacts. Of course, the opposite is true of the NC reed switch, in which the contacts are closed when the magnetic field is

affecting them. If the magnet is removed, the contacts will open.

The magnetic reed switches are set into the doors and windows in each zone, either surface mounted or recessed. Recessed switches (fig. 77) are invisible when the door or window is closed, being set into recesses in the frame. For this reason, they are not as easily tampered with as the surface-mounted reed switches. The circuit will be broken whenever the door is opened, and this will trigger the alarm.

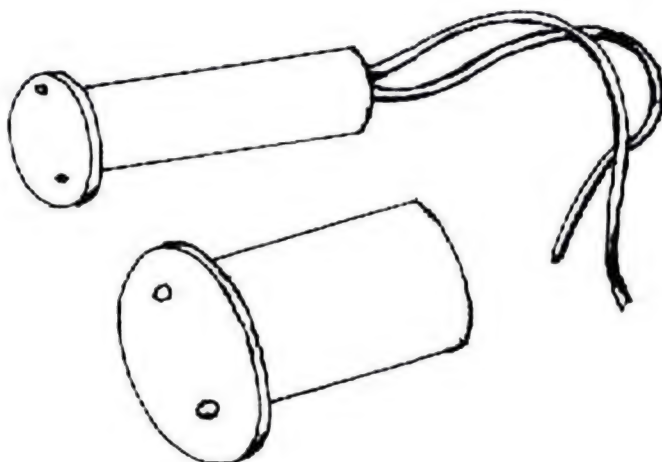


Figure 77. Recessed magnetic reed switch.

The switch is usually mounted in a fixed position, such as a window frame or a door jamb, opposite the magnet, while the magnet is fastened to the window or door. When the window or door is opened, the removal of the magnet will force the switch contacts to change status. This will open or close them, depending on the type of switch. In either case, the alarm will sound.

NC reed switches are the most common, as they are most secure. Of course, NO reed switches can also be used, but, once again, they can be circumvented by simply cutting the wiring.

Magnetic reed switches will be found as far away as possible from the hinges, as they then will trigger the alarm even if the door or window is only partially opened. The switch will generally only be located near the hinges if the

owner wants to open the window at night for ventilation. An ordinary reed switch generally triggers when the magnet is moved away more than about 2 or 3 centimeters, although some switches, so-called wide gap switches, allow the window to be opened 5 centimeters or so. The latter switches are used when the construction of the window or door does not allow the two pieces to be mounted closely together. They are also used if the owner of the system wishes to keep a window slightly open for ventilation.

Reed switches come in different shapes and brands, but they are typically about 3 1/2 to 4 centimeters long and a little more than a centimeter thick and wide. They are, for obvious reasons, always mounted in pairs, one of the pieces (always the one on the moving part of the door or window) housing the magnet and the other housing the stationary switch part mounted on the door jamb or window sill. When the window or door is closed, the two parts will be very close to each other. Look out for the wiring, which is sometimes hidden in the wood. The terminal screws for the wiring will generally be visible, however.

Some alarm systems also include miniature reed switches. They work in exactly the same way as ordinary reed switches but must be aligned properly and placed very close to each other, as the magnet is smaller and the magnetic field consequently not as strong.

Sometimes reed switches can be found in other locations, protecting, for instance, cabinet and cupboard doors, internal doors, or even garden gates.

It should be mentioned that some self-contained window/door alarm systems also rely on magnetic reed switches. The only difference is that the switch section is fully integrated with the control unit. Some of these devices can even double as door chimes when disarmed.

Magnetic reed switches are generally located in a separate loop, as they will only sound the alarm once if the intruder leaves the door or window open after entering. If they are positioned in a loop together with other sensors, this loop can easily be nullified by leaving the reed switch and its magnet well apart from each other. No other sensor

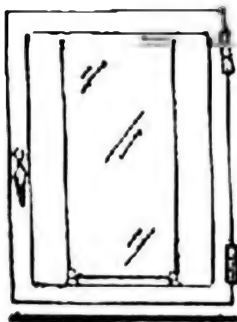


Figure 78. Wire contacts.

can then sound the alarm after it has been sounded once by the reed switch.

Wire contact systems are now very old-fashioned, but they can still be found occasionally. The wire contact switch relies upon a wire or thread that is connected both to the switch and to another, fixed point. The switch will sound the alarm if the thread is either put under tension or slackened. As the thread is generally an electrically conductive wire, the wire will also function as a sabotage alarm. Therefore, the alarm will sound if the wire is cut or broken. Wire systems of this kind are generally used to protect windows and walls (fig. 78) or serve as external alarms in gardens, for instance.

WINDOW FOIL

Adhesive window foil, although nowadays clearly dated as an alarm sensor, is still in common use, especially in shops. It is not commonly used in residential alarm systems. Window foil looks like silvery lead foil and can be found around the edges of the window (fig. 79). The foil

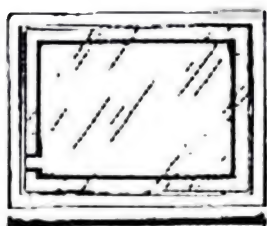


Figure 79. Window foil.

consists of thin metallic strips made of a lead-aluminum alloy, which are cemented to the protected surface, usually glass in a door or window. The metallic strips are connected to a closed electrical circuit. If the protected material is broken, and the foil as well, the circuit opens. This will initiate the alarm. Sometimes foil is simply called tape.

Window foil has many disadvantages. The main one is that a foil alarm is a one-time alarm only. When the window has been broken and the alarm has sounded once, anybody is free to enter until the window and the circuit have been repaired. Another disadvantage is that the foil

deteriorates with age and often becomes too brittle to function after a few years. Yet another disadvantage is that the foil will not sound the alarm if the intruder simply cuts the window open with a diamond, without breaking the foil. Then repair or replacement is necessary. Finally, windows protected by foil generally cannot be opened. For these reasons, other alarm sensors, such as glass breakage detectors, are better investments and are therefore used more commonly.

If the foil is installed on a window that needs to be opened occasionally, it will be connected to a contact strip, which is used to disconnect the wires from the window foil block. The spring section is mounted on the window itself, while the contact plate is on the window sill. The metal tabs on both sides of the switch must make good contact.

The connection between the window foil and the control unit is, under normal circumstances, active only when the window is closed. Window foil is used with the NC circuits of the system. It must therefore be disconnected if the window is to be opened. If so, the switch must be prepared for a coiled jumper wire that will temporarily bridge the gap between the two parts of the contact strip.

There have been attempts to make more reliable versions of window foil. Certain manufacturers of insulated windows include a very narrow and thin metal strip in the glass, usually hidden by the rubber strip used for insulating the window. They reason that the strip will break if the window is broken. This alarm system is more safe, as the metal strip is effectively invisible and securely located, protected by the glass. However, this is also a one-time-only alarm and suffers most of the same disadvantages as ordinary window foil.

WINDOWPANE-MOUNTED GLASS BREAKAGE DETECTORS

Glass breakage detectors (fig. 80) come in several different types, but they all are designed to detect when a window is broken or otherwise removed from its frame. In either case, the sensor is attached to the glass on the inside of the win-

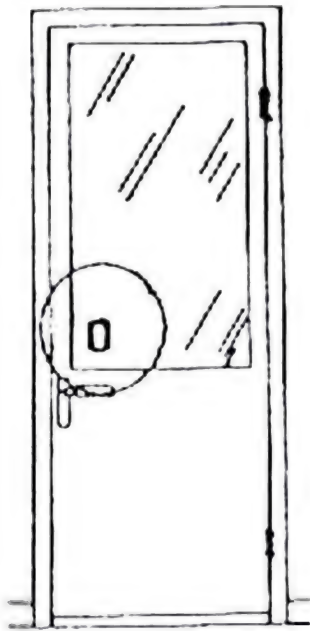


Figure 81. Vibration detector.

dow. The sensor is fastened with double-sided adhesive tape, but it can be removed easily if required. There are versions available both as NC and NO switches. One detector per window is generally sufficient, unless the windows are very large, such as in major offices or shops.

So far, the three most common types of glass breakage detectors include the mercury switch type, the weighted arm type, and the electronic or "tuning fork" type.

The mercury switch type, obviously, relies on mercury. At room temperature, mercury is a liquid metal that conducts electricity. The detector is designed to have a small pool of mercury near an NO switch. If the glass in the window on which the detector is mounted is broken or severely shaken, the switch will be tilted or moved and the mercury will come into contact with the switch terminals. This will close the switch and trigger the alarm.

The weighted arm type uses a movable internal contact that is weighted so it remains in one position. However, most vibrations will make the arm move. This will either complete or break an internal switch contact, depending on how it is designed. The contact will trigger the alarm.

The electronic glass breakage detector uses an internal tuning fork which vibrates when the window is broken or jimmied. The vibrating tuning fork triggers the alarm.

Glass breakage detectors of these types, in the same way as window foil, can use a contact strip if the window needs to be opened sometimes. All of them share the same problem, however. They are susceptible to any vibrations in the window, including those caused by the wind. This might produce numerous false alarms, especially if the window is not installed in its frame tightly. For this reason, other types

of glass breakage detectors have been introduced that work by detecting the sound frequencies emitted by breaking float glass and/or shattered window frames.

This type of detector can detect and identify the special noise that is heard when glass is smashed, when a diamond is used for cutting glass, or when metal hits glass. For this purpose, the detector incorporates a piezoelectric microphone with a resonating frequency within the range emitted when glass is broken. Another option is a microphone sensitive to frequencies above 60 kHz, so that the glass breakage detector is not sensitive to noise in lower frequencies, such as that which results from heavy traffic. The detector is generally fixed to the glass it is protecting, although some can also be put on adjacent walls. The latter type will be detailed in the next section of this chapter.

The kind of glass is important, as the majority of these glass breakage detectors will only react to that of breaking float glass, but not to the sounds of breaking laminated, tempered, or wired glass. Some of these detectors are also susceptible to false alarms, being set off by the sound frequencies of rattling keys or bottles, for instance.

VIBRATION DETECTORS AND INERTIA SENSORS

A vibration detector is one which is placed on walls or window frames to register vibration caused by blows, drilling, or breaking glass (fig. 81). Self-contained units, to be

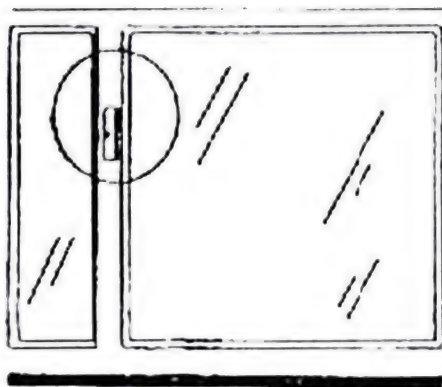


Figure 80. Glass breakage detector.

fixed to doors, are also available. The sensor will signal an alarm whenever it registers the kind of vibrations that it is programmed to identify as signifying an attack. Vibration detectors, or shock sensors, come in different types, some of them relying on mechanical means and others working on electronic principles.

The most common vibration detector is still the pendulum alarm. This is a mechanical detector that relies on a pendulum switch, used to sense vibration or motion. It is designed with a set of NO contacts that come into contact with each other when the switch is moved or shaken. The switch can also be of the NC type, with the pendulum breaking the circuit whenever it is moved or shaken.

Although the sensitivity of these older sensors can be manually adjusted by turning a screw, they have a tendency to produce false alarms. The reason is that low-frequency noise, such as that from heavy traffic and many other sources, will create enough vibration to set off the alarm. For this reason, a new type of vibration detector, the piezoelectric sensor, has been introduced. In appearance, it is similar to the older types.

This is a sensor that is sensitive only to high-frequency vibrations, such as those emitted by breaking objects. The sensor contains piezoelectric crystals, a crystalline material that will develop a voltage when subjected to mechanical stress or severe vibration. The voltage will trigger the alarm. This sensor is often used on walls, windows, and doors. The sensitivity can be adjusted, and the chosen sensitivity will be remembered by a memory circuit. As semiconductors are used, the piezoelectric sensor has no moving parts. The piezoelectric sensor is, in fact, a kind of glass breakage detector but of a type that is not limited to being affixed to the window pane.

Similar devices work according to a different principle. These are acoustical detectors mounted near windows, generally in the ceiling. The detector is then able to guard a number of windowpanes within its range. This detector is sensitive to the noise of breaking glass, shattering wood, and other types of noise signifying a break-in. Its range is often around 15 meters. The detector contains an advanced digital filter, which will ensure that lower frequency background noise will not trigger the alarm. The filter will usually set the lower limit at 5 kHz, but this is often adjustable to between 2 to 10 kHz. Likewise, noise that builds up gradually, such as from cars, aircraft, and vehicle brakes, will not trigger the alarm. This prevents false alarms to a large degree.

The system works on the principle of audio discrimination. This is the process of electronically separating normal everyday sounds, such as voices, telephones, etc., from break-in type noises such as are caused by breaking glass, prying metal, or forcing a door open.

Highly sophisticated sound detectors can easily respond to the sound of a window being smashed. The detector will then respond to the brief time lapse between the sound of the window being smashed and the tinkle of falling shattered glass. Some of these detectors are so sophisticated that they can even distinguish between the sounds of a breaking window and a breaking bottle. There might also be a listening-in function that allows a central security station to listen in on what is happening in the room through the use of an automatic dialer or some similar equipment. This is made possible by the electret microphone built into the sensor. These alarm sensors generally—but not always—work with NC switches.

The most recent type of vibration detector is the inertia sensor. This device looks virtually identical to the other types of vibration detectors. It is an intelligent vibration detector and, consequently, requires a special control unit to analyze the complex signals from the sensor. The principle of this sensor is a comparatively heavy contact element, which rests on a contact surface that is mechanically connected to the cover of the detector. The contact element will not vibrate with the frequencies that are emitted when glass is broken or when metal strikes glass. The rest of the sensor will, however.

Higher frequencies therefore give rise to a burst of short-duration breaks, which are analyzed in the control unit. When the number of short-duration breaks reach and exceed a threshold value, the alarm will be triggered. This will only happen when the vibrations are strong enough to indicate a real break-in attempt. Clearly, determining the likelihood of a real intrusion is a very complicated process, and only a comparatively complex control unit can do so. Therefore, these sensors have other control units in addition to the central control unit of the alarm system.

Inertia sensors are also often found in cars, caravans, and on containers. One such sensor with its special control unit, is sufficient to guard the entire perimeter (i.e., the shell of the construction). When properly installed, the inertia sensor is a very reliable alarm sensor.

INFRASOUND DETECTORS

This is a fairly new type of detector, sometimes used for perimeter alarms in houses and in other relatively enclosed objects, with a floor space not larger than 400 square meters. One detector is sufficient even in a house with several floors, as long as the total area is not too big. It works by detecting sound within the frequency range of 1 to 4 Hz. This is called infrasound, as it is below the sound level normally audible to the human ear. Such sound appears because of the change in air pressure that takes place when a window or a door is being opened. Changes in the air pressure always take place when the enclosing material changes its nature.

It is perfectly possible to move around in the building when the alarm system is armed, as long as no door or window is opened. As only one sensor is necessary, this alarm is very quick and easy to install.

The disadvantage of this system is that it is a one-time alarm only. If an intruder leaves the door or window open, the alarm will only sound once—when the door or window is first opened. Infrasound detectors are therefore usually used with other types of trap alarms.

The infrasound detector can be hidden almost anywhere—under a staircase or behind a cupboard or a curtain, for instance. A good sensor of this type will automatically compensate for natural infrasounds, such as those emanating from strong winds.

FIELD EFFECT SENSORS

The field effect sensor relies on the principle of capacity changes between the guarded object and earth or between

extended conductors or foils. In effect, it works like a radio transmitter and receiver.

If somebody is moving in the field between the transmitter and the receiver, there will be interferences in the received signal. This will trigger the alarm. For this reason, these sensors are sometimes known as field disturbance sensors.

Capacity changes can be indicated in different ways. If a metal safe is to be protected, it can be connected to a frequency-determining resonance circuit. This resonance circuit will control an oscillator, whose output frequency will be compared to a fixed frequency within the range of 100 kHz to 10 MHz. The variations in frequency will be detected and analyzed. If a predetermined threshold value is exceeded, the alarm will sound.

Likewise, a building can be fitted with two encircling conductors, approximately 1 meter apart. One will be the transmitting antenna, in effect the antenna to a long wave radio transmitter, while the other will be the receiving antenna (fig. 82). The system will detect and analyze the differences in the received signal caused by an intruder approaching the protected area.

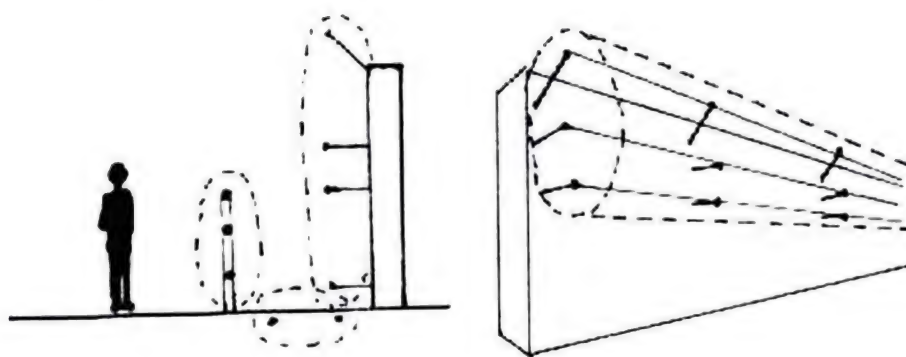


Figure 82. Field effect sensors.

Field effect sensors generally consist of two or more wires running parallel along the protected area. The wires will be connected to the wall or fence by insulators. Particular care will have been taken to position the wires far away from other metal objects, as such objects may limit the range of the detector. Walls, internal walls, corridors,

and other locations can be protected in this way. In a corridor, for instance, the two wires up to approximately 300 meters long will run one on each side. Alarm systems of this type will definitely be more common in the future, and they already exist in many places.

Another variant is the capacitance detector. Such a detector often consists of a metal plate on which the protected object is positioned. If an intruder approaches the object and the metal plate too closely, the electrical capacitance in the plate will change and trigger the alarm.

SOUND DETECTORS AND HEAT DETECTORS

Freestanding, portable sound detectors can be placed almost anywhere and are extremely easy to activate. Some suspicious individuals put one on a table before they go to bed. The sensor will listen for intruders in the room where it is located, and possibly adjacent rooms, too, as long as the internal doors are left open.

Sound detectors are very prone to false alarms, however. The problem is basically that they are too good. They can be triggered by perfectly ordinary noise outside the pro-

ected area, for instance, in the street. The most common type of sound detector is the previously described glass breakage detector.

Sound detectors are often mounted on safes. They sound the alarm if some-

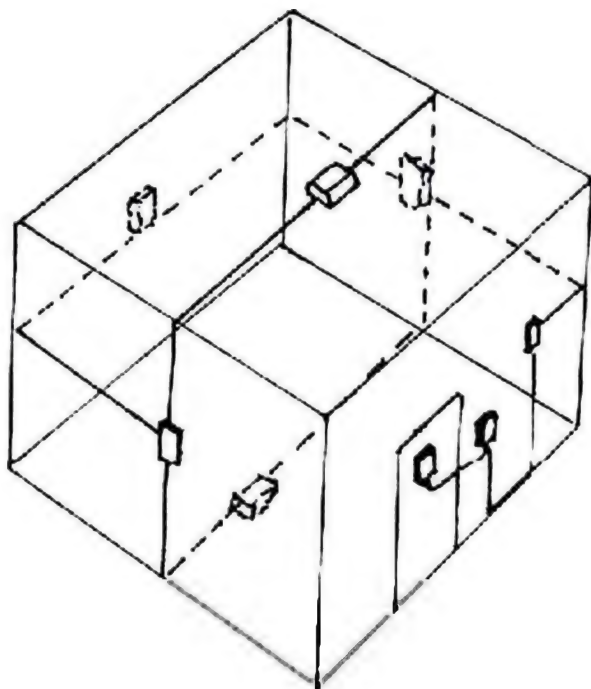


Figure 83. Sound detectors mounted in a bank vault.

body is working on the safe in an attempt to crack it. This detector consists of one or more microphones connected to an amplifier, programmed to only respond to the type of noise expected to signify a break-in. This will ensure that the occasional noise of a broom or vacuum cleaner hitting the safe during cleaning will not trigger the alarm. The microphones are attached to the object with a strong magnet, and a plunger switch or magnetic reed switch sabotage alarm is included, so the alarm will sound only if somebody attempts to remove the detector from the object. Sound detectors are commonly used in bank vaults and are mounted on every wall, as well as in the floor and ceiling (fig. 83).

A sound detector is often mounted on a safe along with a heat detector. This device should not be confused with the infrared detector. The heat detector will only register the heat of a welding torch or a fusing burner.

PRESSURE MATS, PLUNGER SWITCHES, AND CONTACT STRIPS

Pressure mats (fig. 84) look like rubber floor mats and are commonly hidden under wall-to-wall carpet and

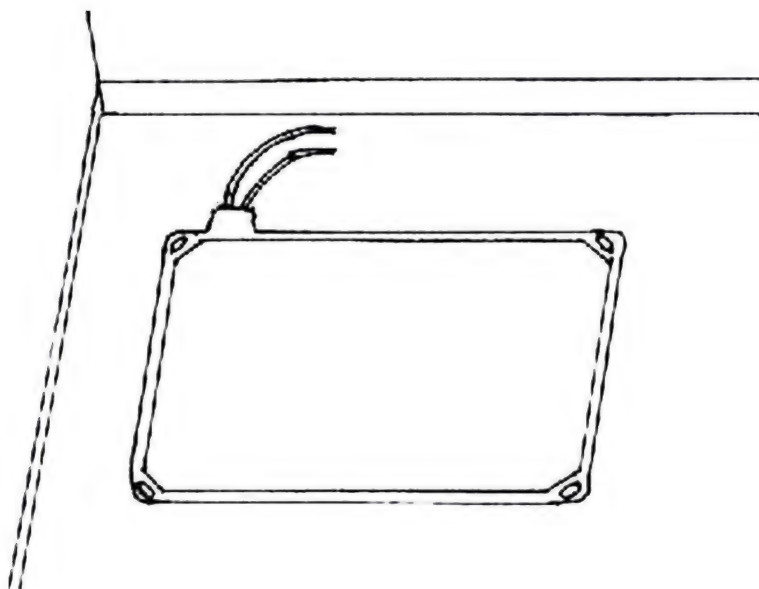


Figure 84. Pressure mat.

linoleum floors at strategic places in the building (e.g., in front of certain doors and windows, at the foot of the stairs, or directly in front of a safe or important object). It is also common to use a series of pressure mats in a staircase, so that it is virtually impossible for an intruder to avoid stepping on at least one of them if he wants to proceed to the next floor. As staircases are often of different sizes, the pressure mat also comes in several different sizes.

The pressure mat is in fact a large NO switch. The mat contains two grids of switch contacts separated by a non-conductive material that has been perforated several times. The contacts can be brought together through the holes. The contacts are only pressed together when a person of sufficient weight (i.e., a person; children will trigger the contacts, but not pets such as cats or small dogs) steps on it. Then the NO switch is closed and the alarm triggered.

If the pressure mat is hidden in an unsatisfactory way, the outline of it might start to show through the carpet after a long period of use. The intruder can then avoid it easily. Certain inferior brands of pressure mats will also be triggered by pets such as cats or dogs, so the presence of these animals might indicate the absence of pressure mats, at least in older or less secure buildings.

A plunger switch is a mechanical device located on doors and windows to detect entry or tampering (fig. 85). It is an ordinary spring-loaded momentary switch that is designed for use in

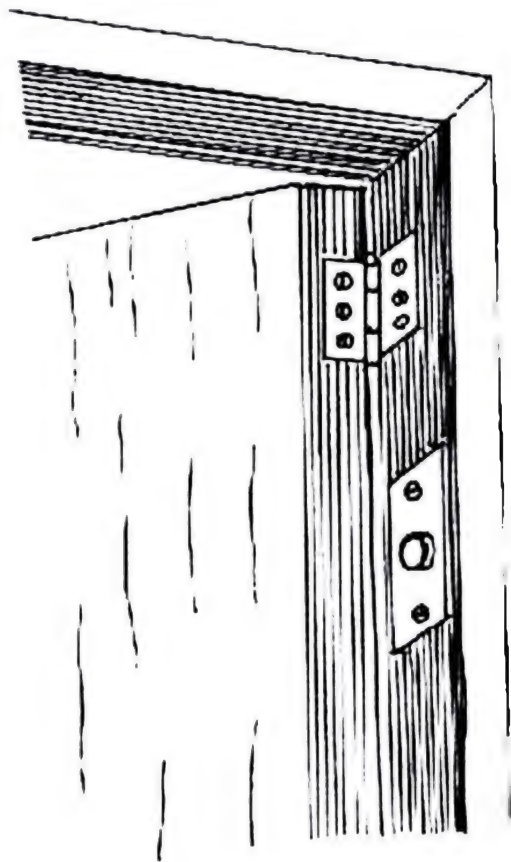


Figure 85. Plunger switch.

alarm systems and has a depressible plunger or button. The plunger in itself is oversized, while the body of the switch is designed for mounting on doors, windows, or control units. The plunger switch is easy to bypass, as long as it is known to exist. Simply keep the plunger under pressure with a piece of celluloid, for instance, so that the device does not indicate an alarm while you are removing the switch from the protected area.

The plunger switch is often used in control units to prevent the system from being tampered with. In this application, switches will be mounted on the front and/or back of the control unit. The alarm will sound if the door is opened or the control unit is removed from the wall. Here it is more difficult to remove the switch because of its location.

In the same way, plunger switches can be used to detect when a door or window is opened. In this case, the switch is mounted so that the plunger will be depressed when the door or window is closed. The switch is then mounted on the hinge side in the door jamb and is virtually impossible to see, as it is neither exposed from the inside or the outside when the door is closed. Of course, this type of switch is an NC switch. Whenever the door is opened, the alarm will sound.

A contact strip mechanism is, in effect, an open switch and is sometimes used on windows and doors, usually together with window foil and glass breakage detectors.

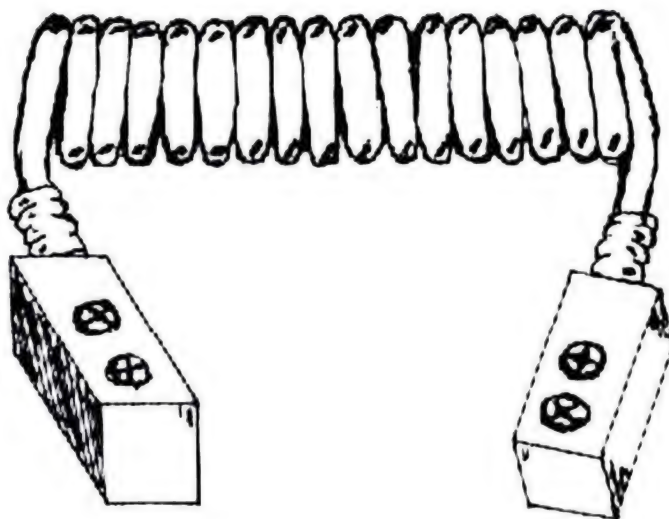


Figure 86. Contact strip bridged with jumper cord.

The contact strip is similar in shape to the reed switch and is also composed of two parts. Here, too, one part is mounted on the window or door, while the other is mounted on the frame (fig. 86).

The advantage of the contact strip is that the two pieces can be bridged together with a jumper cord. This is highly useful when a window or door (e.g., a garage door) must be left open but the alarm system is still armed.

IONIZATION DETECTORS

The ionization detector is not used anywhere yet, as far as it is known, but this might well be the alarm sensor of the future.

The ionization detector works according to the principle of the Kirlian effect, which states that living matter is surrounded by a "force field" that ionizes the surrounding atmosphere. This will produce an aura, or halo, around a living being photographed in fields of electrical current. (The Kirlian effect is not universally accepted, as the reason for this phenomenon is so far unknown. The phenomenon has also been abused frequently by sensation-seeking parapsychologists. However, this has not prevented research in ionization detectors.)

The ionization detector will work in the following way. It is well known that if the atmosphere is ionized this will change the electrical conductivity. An ionization detector will therefore register the atmospheric conductivity. Any changes resulting from the ionization of the surrounding atmosphere that is caused by the "force field" around a human being will be detected.

No known alarm systems rely on this principle today, but in what was formerly the Soviet Union, the Kirlian effect has been accepted for several years. It is probably only a matter of time before sensors of this type are in production.

PHOTOELECTRIC CELLS AND INVISIBLE BEAM DETECTORS

Photoelectric cells have been in common use for years, especially in shops, to detect a person walking into a room

or through a door. Old-fashioned systems of this type use visible light, and the person entering has no trouble at all noticing and evading the photoelectric cells should he choose to do so. Nowadays, what is basically the same system is still widely used, but instead of visible light, invisible infrared light is used.

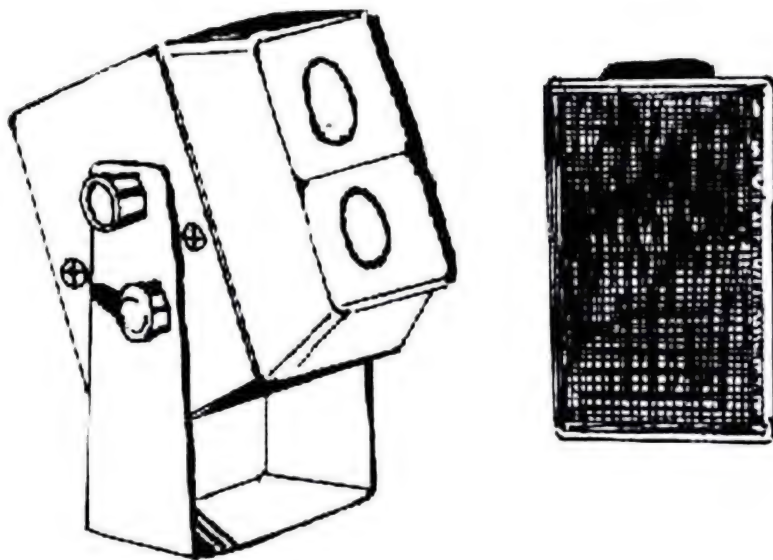


Figure 87. Photo relay sensor with detector (left) and the reflector (right).

The modern invisible beam detector, or photo relay sensor (fig. 87), is designed to project a narrow infrared beam across the area to be protected. For this reason, sensors of this type are also sometimes called active IR-detectors. The beam is aimed onto a small reflector, which will reflect the infrared beam back to the invisible beam detector, which has a built-in photoelectronic eye that is sensitive to infrared light. This photoelectronic eye will constantly monitor the area, and as soon as somebody interrupts the beam between its projector and receiver, either completely or almost completely, the alarm sounds.

Most invisible beam detectors of this kind are able to protect an open area up to about 10 meters wide. Larger units, however, are conceivably capable of a range of several hundred meters. These units are commonly used outside a building, in a private garden or park, for instance (fig. 88). Sometimes they are used to protect rooftops as well. With

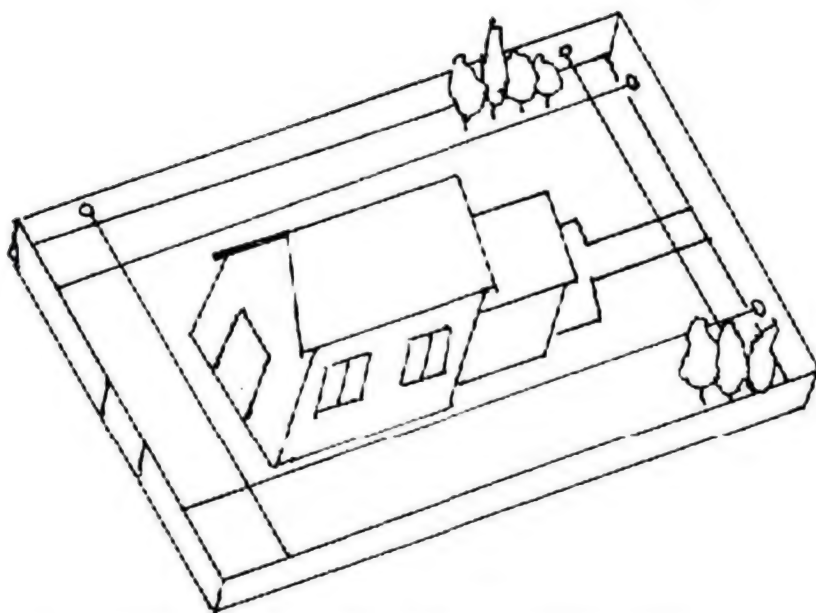


Figure 88. Infrared beams arranged for perimeter protection.

the exception of really sensitive installations, these detectors will generally trigger security lights rather than sirens, as the chance of false alarm is very high.

The most common method of installation is with two invisible parallel beams. Then a small animal such as a bird will not trigger the alarm, but a human-sized intruder will break both beams and trigger it. Likewise, mist or falling snow, rain, or leaves will not trigger the alarm. The range is generally up to 150 meters, but it is shorter in countries with cold climates. Many detectors of this type can function even if covered by snow or frost, however.

The emitted infrared light is modulated so that the receiver can identify it without being disturbed by other

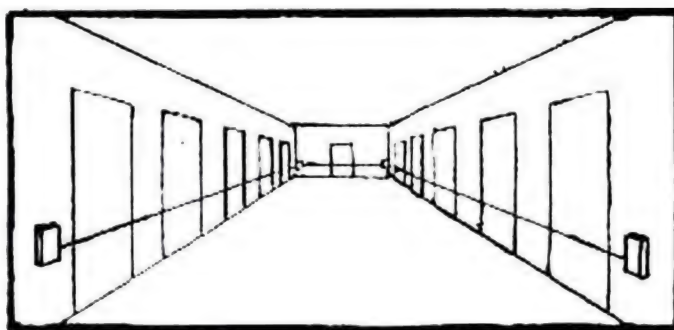


Figure 89. Infrared reflectors used to protect a corridor.

sources of infrared light, such as sunlight. The infrared beam might also be reflected by infrared reflectors (fig. 89), which will increase the range even more. As the invisible light used in the beam consists of infrared light, these detectors can be found and evaded easily by using infrared-goggles during the entry operation.

PASSIVE INFRARED DETECTORS

A passive infrared detector, or PIR as it is commonly known in Britain and some other countries, is a device that receives and measures infrared energy from other objects. It is, in effect, a heat detector, although it is of a very different type than the heat detectors mentioned earlier in this chapter.

The passive infrared detector is usually fixed high on the wall, either in a hall or in a large room which must be traversed to reach the sensitive areas. It works by picking up an intruder's body heat, triggering the alarm whenever it detects body heat within its range. The detector is extremely sensitive and will pick up even the smallest variation in temperature, both above and below normal.

The passive infrared detector works by utilizing a built-in pyroelectric sensor. Simply speaking, this sensor is able to indicate heat by producing an electric charge. The pyroelectric sensing material is polarized by infrared radiation producing a voltage proportional to the rate of change of incident energy. The pyroelectric sensor will electronically monitor the room protected by the alarm. It is surrounded by a reflective surface that collects infrared energy. As the sensor is sensitive to heat (i.e., infrared energy), it will sense any change in the level of infrared energy, including the presence of any intruder radiating heat. Such an abrupt change, such as is caused by the appearance of an intruder, will be readily detected and will trigger the alarm.

A resting human will radiate approximately 100 W, so we are all major sources of infrared radiation. However, mere radiation is not enough to trigger a passive infrared detector. The heat source must also be moving through the zone monitored by the detector.

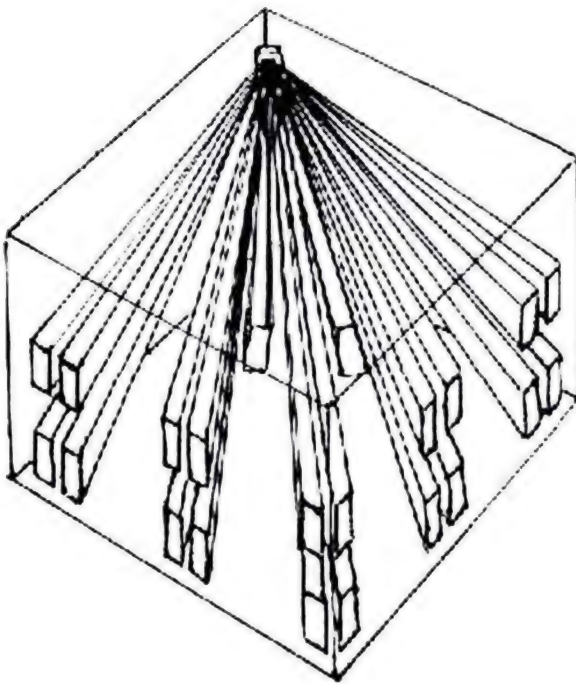


Figure 90. The detection zones of a passive infrared detector.

The passive infrared detector will divide the area to be monitored into zones and segments (fig. 90), typically up to 7 meters across (actually 76 degrees wide, usually, but this can vary), 12 meters deep, and around 70 centime-

ters high. Only these zones and segments will be monitored, and intruders above or below them will not be detected. The detector must therefore be adjusted very carefully during installation to ensure maximum protection as well as to prevent false alarms triggered by pets or small children. For these reasons, it will generally be positioned at the level of a man-sized intruder's head or higher—at least 1 1/2 meters above the floor. The detector is most often positioned along a wall or in a corner so that it can have a free line of sight to as much of the room as possible, including the front door, if at all feasible.

A passive infrared detector typically looks at a zone of six or more separate segments with unwatched "aisles" between them. A separate-zone design gives the unit wide-angle coverage of a room. As the background radiation of each zone is slightly different, it is virtually impossible for an intruder to match them all.

Self-contained infrared sensors generally cover a wider area and have more zones but typically protect an area up to only 8 meters deep. There is also a lower zone in each segment. This will usually ensure that an intruder cannot

slip under the monitored zone. Sometimes, especially if pets are on the premises, the lower zone will be turned off.

There are also infrared detectors on the market that can monitor areas up to 50 meters in length. The range of some of these can be varied if the owner changes the lenses.

The IR-detector is prone to false alarms, however, as it will be triggered not only by obvious problem sources such as cats and dogs, but also by small pests or bright sunlight through a nearby window. Even being too near any quick-changing source of heat or cold, such as a central heating radiator producing radiated heat and warm draughts or an air-conditioning duct, might produce a false alarm.

When an infrared detector is switched on, it first balances itself based on the amount of background infrared radiation coming from various sources in a room, such as walls, furniture, and floors. If an intruder later enters the detection zone, he alters the amount of infrared radiation detected. This results in an alarm.

This need to first balance the sensor means that if the power has been switched off for some time, the sensor will require approximately ninety seconds to be operational. However, this is not necessary when the system has merely been disarmed but has retained its power.

In addition, the detector will not respond to slow variations in background radiation because amplifying circuits limit the detectable variations to a predetermined range of possible speeds.

In advanced units of this type, a threshold circuit will also ensure that a signal is large enough to represent an intruder. In this case, a pet will not trigger the alarm, as long as it is not very close to the detector. Of course, the sensor's sensitivity to false alarms is also determined by the positioning of the detector and its segments of protection.

Every infrared sensor will be most effective in detecting movement across the segments, rather than movement toward or away from them (fig. 91). There have been lab tests to determine the possibility of making a very slow direct approach to the sensor so that it will not feel a sharp increase in temperature and, consequently, refrain from sounding the

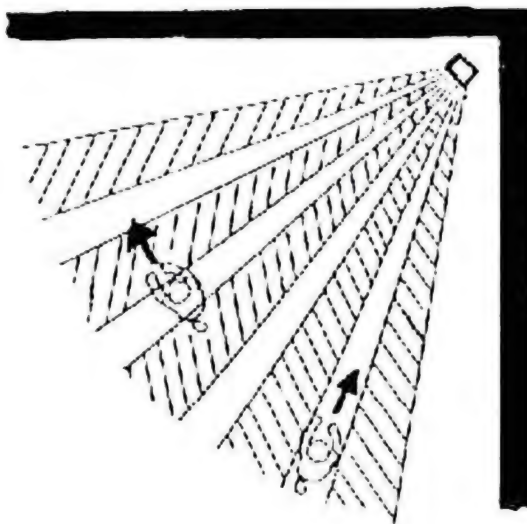


Figure 91. The passive infrared detector is most sensitive to movement across its segments.

alarm. In some of these tests, the "intruder" was hiding behind a thick glass pane, as plain glass will absorb a considerable portion of the radiated heat. However, no such experiments have

been deemed successful enough to warrant the use of the techniques involved in the field.

An infrared detector can also be mounted in the ceiling. If mounted as high as 6 meters, the protected area will be as large as 6 x 20 meters, and all movement will naturally occur across the segments. This facilitates detection.

Passive infrared detectors, although generally used to monitor movement in rooms or along corridors, can be used vertically to create an alarm curtain, in front of a wall of paintings, for instance. They can naturally also be used to create a horizontal curtain to detect a break-in through the roof, ceiling, or floor.

Most passive infrared detectors have built-in tamper switches to prevent somebody from removing the unit from the wall or attempting to disarm it. Infrared sensor systems, whether self-contained or part of a separate-components system, are easy to locate. The sensor is generally positioned so that its zones of detection include the expected entry, such as doors and windows. The intruder should be forced by the layout of the building to walk into these zones. Furthermore, the sensor will be placed at least 1 1/2 meters above the floor. This is necessary if the lower portions of the zone are to be used.

The sensor unit will be positioned so that its field of view does not include solar-heated walls, direct sunlight, heaters,

air conditioners, or other objects that might change its temperature quickly. The older infrared sensors might produce false alarms under these circumstances. Contemporary models will not do so as readily, but their detection ability will be impaired somewhat. In the contemporary models, every segment is divided into two channels. The detector will only sound the alarm if the change in temperature is different in both channels. This will prevent the alarm from sounding when a radiator heats up, for instance. An intruder, however, will first disturb one channel and then the next, thus triggering the alarm.

Self-contained infrared sensor systems incorporate entry and exit delays, typically fifteen to twenty seconds in length. Otherwise, a remote key switch might be used. Backup batteries can also generally be connected, as can external warning devices.

There are also smaller, self-contained infrared detectors. They generally work with only one coverage zone and are supposed to guard only small areas near doors, windows, trailers, etc. If a heat source is detected, the built-in siren will sound for about one minute, after which the unit will reset. An entrance and exit delay of a few seconds is generally built into these units. Power is generally provided by a standard 9-volt battery located inside the detector unit.

MICROWAVE MOTION DETECTORS

A microwave motion detector is a trap alarm with a single-unit transmitter/receiver that reacts to distortions in the timing of its return signal. The device works, in effect, like a small radar system, using an electromagnetic field comprised of high-frequency radio waves generated over the protected area. Most detectors of this type have a range of 30 meters or less.

The microwave motion detector relies upon microwaves, very high-frequency radio signals in the range of around 9 GHz. These radio waves will form a pear-shaped lobe (fig. 92) that will detect any intruder. As these microwaves are reflected off solid objects, they will reveal the presence of an

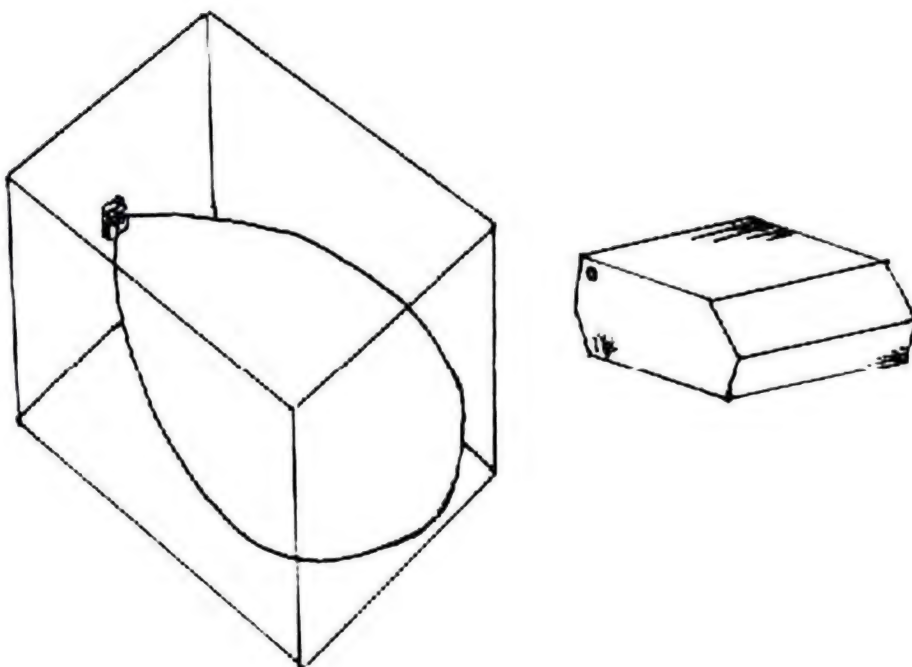


Figure 92. Microwave motion detector and its detection zone.

intruder entering the protected area, as his movements will cause a disturbance in the reflected radio waves (i.e., the radiated RF field sensed by the device).

This disturbance is a modulation of the field referred to as the Doppler effect. The Doppler effect is the difference in frequency of one (original) wave to another (reflected) wave that is superimposed upon it. The reason for this is that a frequency shift occurs when a signal source and a receiver are moved relative to each other. According to the Doppler effect, the reflected signal will be of a lower frequency than the emitted signal if a reflecting object or a human is moving away from the detector. Likewise, the reflected signal will be of a higher frequency than the emitted signal if a human is approaching the detector. The reason for this phenomenon is that since the signal moves at a constant rate, the return trip of the reflected signal should take the same length of time as the outward trip. However, an intruder who moves into the path of the signal distorts the timing of the return signal. This frequency shift is sensed by the microwave detector unit's receiver. Whenever it detects

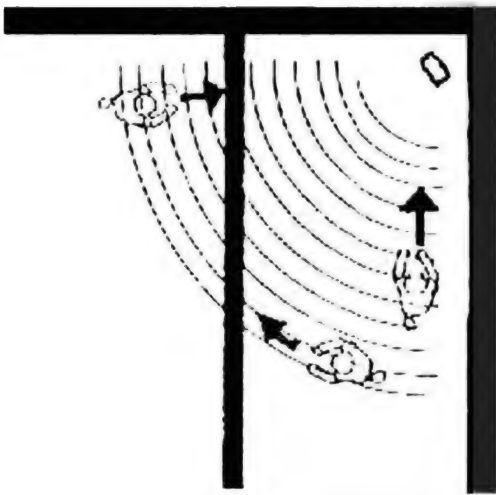


Figure 93. The microwave motion detector is most sensitive to movement toward or away from it. Note that it is also sensitive to movement in another room.

such a change in the reflected signal, the unit will trigger the alarm.

As the frequency of the microwaves is very high, the wavelength is

very short. This means that even a very small movement will result in a large frequency shift. However, the detector is less sensitive to objects moving across its field of detection than it is to objects moving toward or away from it (fig. 93).

Most microwave detectors require that an intruder move at a certain speed in order to be identified as an intruder. These detectors are able to reject faster-than-walking speed. This will prevent numerous false alarms, as many microwave motion detectors, especially the older models, work all too well. As their signals can penetrate beyond the walls of a house, they might identify a passing truck as an intruder, for instance.

External radio sources can also trip these units, as the RF energy radiated by many electrical devices will disturb their functioning. Such electrical devices include radios, especially citizen band radios, but also cable television systems, motors, transformers, and even neon signs and fluorescent lamps. The gas in such lamps, when switched on, ionizes to become a fluctuating reflector which can easily cause an alarm. A false alarm might also be caused by cooling fans and sometimes even the roof in a warehouse, if the roof rises and falls in the wind. The movement of water in pipes might even trigger a false alarm, as the sensor has the ability to see through glass and thin walls of plaster or plastic.

As the microwave motion detector is an extremely small

radar, the microwaves are completely harmless, unlike the radiated energy from a large radar such as is used for air traffic control or military purposes. There are also microwave/passive infrared detectors. They are very reliable, as the two sensor types complement each other well. The microwave detector determines that the object moves within a certain range of speed, while the infrared detector checks whether the object emits heat or not. These combination detectors come in different types, with ranges up to 65 meters.

ULTRASONIC MOTION DETECTORS

An ultrasonic motion detector is a single-unit transmitter/receiver that signals an alarm when its steady pattern of inaudible sound waves is disturbed. It works in a similar fashion to the microwave sensor, but it uses ultrasonic sound waves instead of microwaves. The principle is still the same as that of radar.

The ultrasonic detector works by continuously transmitting ultrasonic sound waves of such a high frequency, around 40 kHz, that a human cannot hear them. The typical upper limit of human hearing is twenty thousand cycles per second, or 20 kHz. The ultrasonic sound waves are therefore well beyond the human range of hearing.

The sound waves will bounce off the hard surfaces in the room, in effect producing an echo which, thus reflected, will be picked up again by the same unit. An intruder entering the room will interfere with the frequency of the reflected sound. Because of the Doppler effect, the reflected sound waves will experience a frequency shift if they are reflected from an intruder entering the protected area. When the intruder moves within the field, the unit's receiver detects a change in the reflected signal and triggers the alarm.

Because of the nature of sound, the ultrasonic detector will produce a teardrop-shaped "cone" of ultrasonic energy, similar to what is illustrated in Figure 92. This cone will expand horizontally and vertically away from the unit across a relatively broad area, typically up to 9 or 10 meters

in a forward direction and up to 7 meters wide. However, the shape and size of the cone will vary with the acoustical characteristics and shape of the room in which the sensor is located. Walls and glass windows will not be penetrated, except to a minor extent. There are also ultrasonic detectors that work with separate transmitters and receivers. They often have a longer range.

The ultrasonic detector is most sensitive to movements

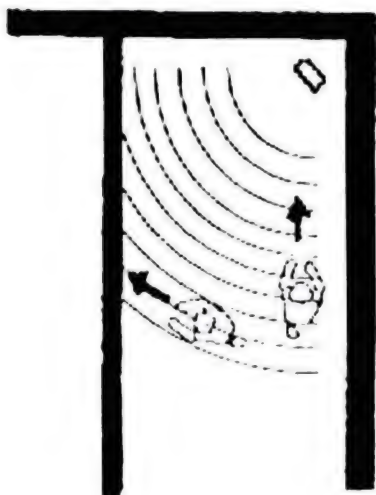


Figure 94. The ultrasonic motion detector is also most sensitive to movement directly toward or away from the sensor.

directly toward or away from the sensor (fig. 94). This is unlike the passive infrared detector, which is most sensitive to movements across its protected area, but similar to the microwave motion detector. The reason, of course, is that both of these types of detector rely on the Doppler effect. Ultrasonic detectors are therefore used more commonly for protecting doors and hallways than are passive infrared detectors.

Ultrasonic detectors are usually located in the corner of the room to be protected, fixed to the wall, or else aimed

down a hallway or at an entrance, such as the front door.

These detectors are fairly prone to false alarms, which might be produced by loud noises, such as ringing telephones, as well as moving objects, such as draperies near vents or fans. Even air currents, draughts of moving air from heating or cooling vents, and other types of air turbulence can produce false alarms. For these reasons, most ultrasonic detectors include a control for adjusting the sensitivity of the device. The ultrasonic detector cannot be used if pets are present, though, as there are no unprotected areas within the coverage zone.

Many ultrasonic detectors have a delayed alarm, which

makes the intruder's first steps into the protected area appear to go undetected until it is already too late.

Because of their tendency to produce false alarms, ultrasonic detectors seem to be decreasing in popularity.

VISIBLE LIGHT DETECTORS

Visible light detectors are not common, and they can only be used in certain locations. They are mainly used in conjunction with other detectors in bank vaults. The detector will simply sense if the level of visible light in the location is rising. If so, it will sound the alarm. (The bank vault is, of course, supposed to stay dark when closed.) A detector of this kind is of a very simple design. The visible light detector can only be used in closed locations where no natural light can enter.

VIDEO DETECTORS

A video detector constantly monitors the object it is guarding by merely "watching" it. The detector, a modified video camera, checks the level of black (the number of black dots, opposed to the number of white dots, in a picture) in certain interesting areas of the video input. If this level is changing slowly, the detector will not trigger the alarm, as this might indicate sunset, for instance. However, a drastic and immediate change will trigger the alarm, as this means that a person or an object has entered the field of vision and is now near the protected object.

Video detectors are reliable but fairly expensive. For this reason, they are not widely used as yet. They will probably be more common in the future, particularly since it is also possible to transmit the video signal across the telephone network by means of a modem. Then a remote control station can view and interpret the video.

The latest detectors of this type are even more advanced than the standard video detector. A number of cameras can be used to constantly monitor the zone to be protected. The video output from each camera will then be processed by

an intelligent image processor based on neural network technology. This will automatically identify any intruder.

The system works by first learning the characteristics of the natural state of the environment under observation, including moving items such as shadows, branches of trees, or level crossing barriers. This initial learning state does not need to last for more than a minute. The system can even be taught to ignore certain dynamic events, such as guard patrols or vehicular movement.

When the system enters operational mode, it identifies intruders within its field of view by recognizing abnormal patterns of movement. It immediately sounds the alarm and automatically trains a high-resolution camera onto the target for identification and video recording purposes.

This advanced system is not yet in widespread use, but it can be found in certain British defense research installations. It can also be configured to be portable. Expect it to be common in most high-risk installations in the future.

BARRIER SENSORS AND ANALYZERS

A perimeter barrier is a wall, fence, or gate marking the perimeter of the property. Guarding such a perimeter, especially if large distances are involved, requires special sensors and sometimes also special control units or analyzers.

Today, the most popular barrier sensor is the inertia sensor, even though there are various other types on the market. The inertia sensor, used in conjunction with a special barrier analyzer, can be adapted easily for use on any fence.

The inertia barrier sensor system is an electromechanical system that relies on special wires (fig. 95). Every wire is connected to a special self-adjusting sensor installed in a sensor post, or pole. The sensor is positioned between two horizontal wires that run between the sensor posts. The sensor will notice immediately any attempt to spread the wires (to enter between them), climb on them, cut them, or otherwise remove them.

The sensor-connected wires are fitted with vertical springs and self-adjusting connection points so that they

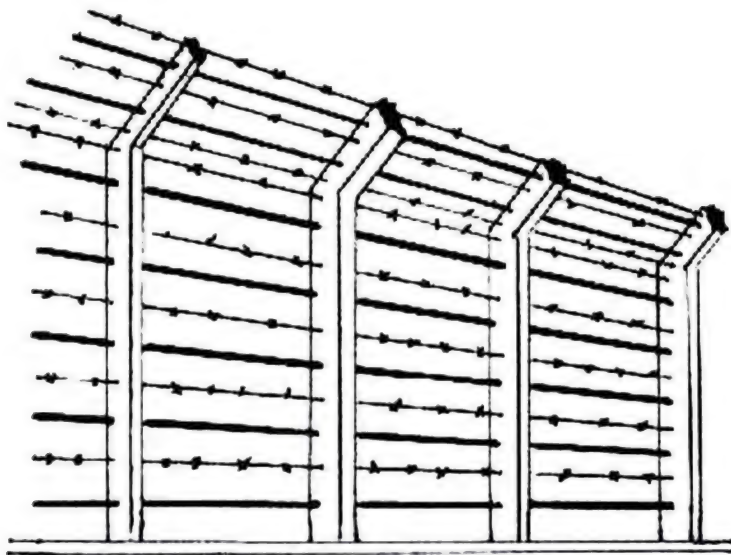


Figure 95. Inertia barrier sensor used on a fence.

will detect any kind of intrusion. Six wires and sensors will generally be fixed parallel to each other on the posts so that it is impossible for an intruder to avoid all of them if he is attempting to enter. This also allows the system to determine the exact height of an intrusion. Another advantage is that a wire group can be disconnected, during maintenance, for instance, without the rest of the sensor post being affected or impaired.

The sensor posts are generally positioned up to 50 meters apart, although a shorter distance, say 10 meters or so, will make the system able to really pinpoint an attempted intrusion. The sensor posts are made of aluminum or stainless steel, unlike the ordinary posts that are made of stainless or galvanized steel. Every sensor post has individual tamper protection and is also monitored individually by the computer in the central security station.

A multiplex computer communications system will keep in touch with every single sensor post and wire through a special information cable that runs along the fence. Every detected intrusion will then be reported by a special reporting unit in each sensor post and will be monitored and registered by a computer in the central security station. The system will also self-test continuously, sound-

ing an internal alarm if any part of it breaks down or is subjected to attempted sabotage. Naturally, this self-test also includes the information cable. In addition, every incident will generally be logged in the central security station computer if the need arises later to verify what happened.

The computer communication will go in both directions, which means that individual security measures can be adopted in case of an alarm. These might include video cameras and searchlights or armed mines programmed to be activated automatically, without the need for a manual operator.

As can be readily imagined, this type of system is very complex and only used in high-risk locations. The most famous system of this type is the Israeli Magal system. Magal Security Systems now guard the entire length of Israeli border fences and barriers. An identical system, also produced by Magal, is used in numerous other countries, in military installations and around nuclear power plants, for instance. The best way to circumvent this alarm system is to avoid touching the fence. Try to enter in another location or from the air.

Another common sensor used to protect a perimeter is

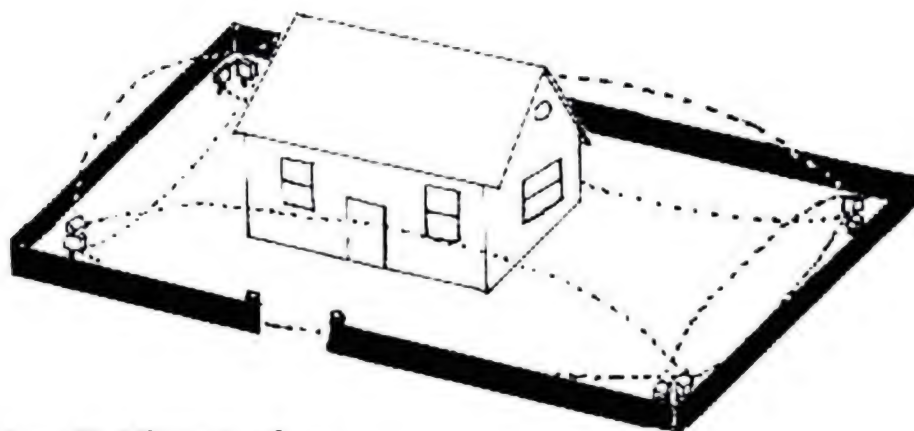


Figure 96. Microwave fence.

the microwave fence (fig 96). This is, in effect, a radar barrier and works by a transmitter sending a pattern of invisible microwaves to a separate receiver, located up to 300 meters away. Any intruders crossing the path between transmitter

and receiver will distort this pattern and the alarm will then be signaled.

Transmitters and receivers can be positioned along the perimeter of a garden, for instance, or any other open area. The microwaves will create a signal field, which might be between 2 and 8 meters high and up to 20 meters wide or more.

This sensor is very prone to false alarms, as there is no way of distinguishing between an intruder and an ordinary bird or animal. Even moving vegetation might trigger it. It will, however, detect even small changes, so an intruder crawling slowly into the field will be detected. The sensitivity is adjustable, however, and some systems of this type will only indicate an intruder that is at least walking slowly. The speed of movement that the sensor can detect can usually be adjusted to between .01 and 10 meters per second.

As the transmitter and receiver will be connected by a synchronizer cable in order to force the receiver to notice only its dedicated transmitter, the system can be sabotaged by cutting this cable. However, this will generally also trigger the sabotage alarm. The system cannot be sabotaged by simply transmitting microwaves of the correct frequency into the receiver, as the synchronizer will reveal this as an error.

Microwave barriers are generally fenced in, as the presence of wild animals would otherwise give rise to frequent false alarms.

Yet another device used for external alarms is the geophone (fig. 97). This is a device that monitors vibrations. It can be installed to detect activity across the ground or the vibration caused by the scaling or attacking of walls and fences. The sensor is, in effect, a vibration sensor.

An older and cheaper barrier alarm system relies on mercury switches as fence alarms. The switches are mounted on the fence and will sound the alarm whenever the fence is moved by somebody climbing it or leaning a ladder against it. The mercury switch is also a vibration sensor, although of an older type. A mercury switch fence can also be circumvented by not touching the fence.

Field effect sensors can also be used as barrier alarm sensors. The system will then use wires connected to the

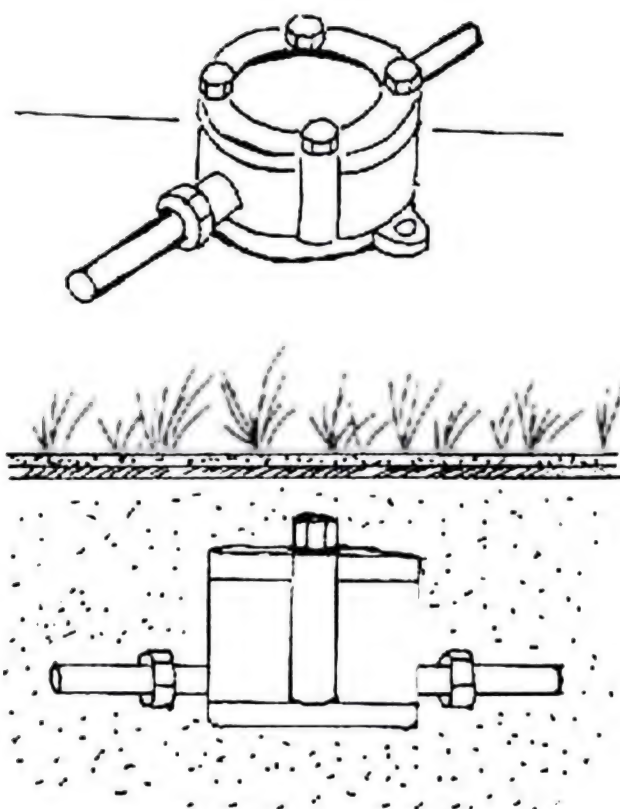


Figure 97. Geophone.

top of the fence. Otherwise, it is the same as the field effect sensor detailed earlier in this chapter.

Yet another system is the cable detector. Cable detectors consist of special cable that is capable of changing resistance or capacitance when bent or hit. The cable will run through the important parts of the fence. It will trigger the alarm if it is bent, climbed on, or cut by an intruder in order to facilitate an entry. Any such movement of the fence will cause a capacitive change in the cable that will in turn trigger the alarm.

Another fairly reliable system uses a thin tube or hose connected to a microphone. The signals from the microphone will be analyzed by an advanced electronic circuit. Any attempt to climb or destroy the fence will be recognized and trigger an alarm. The microphone can be connected to a loudspeaker and monitored in an alarm control station.

All sensors of this type frequently produce false alarms.

Both animals and strong winds that cause the fence to move might be causes. These are therefore usually connected to the control unit separately from other types of sensors, so that the entire alarm system is not tripped just because of an indication from the barrier sensor.

Other Types of Alarm Systems

DELIBERATELY ACTIVATED ALARM SYSTEMS AND PERSONAL ATTACK ALARMS

A deliberately activated alarm, or a panic button, as it is often called, is a device designed to set off the alarm when the individual in charge of the alarm feels threatened or is under imminent attack. Panic buttons are always fixed in place, in a bedroom, for instance, or at the teller's position in a bank.

A personal attack alarm is used for a similar purpose, but this device is not fixed to a certain location. Rather, it is carried on the person to be protected by it and is activated by him or her wherever he might be on the premises. Personal attack alarms are, for instance, often carried by medical personnel who regularly have to deal with potentially dangerous patients. They are also sometimes carried by elderly people who fear that they will be attacked by burglars.

Most professional alarm systems, whether for use by private individuals or by corporate or government offices, include one or more panic buttons or personal attack alarms. Alarm systems in private homes might have two panic buttons, one by the front door and another by the bed. Office alarm systems might have any number of these protective devices.

Regardless of the variety of these alarms available, they all work in the same way. The panic buttons are wired to a circuit on the alarm system that is always live, whether or not the alarm has been switched on at the control unit. The user need only press the button at the first indication that an intruder is trying to enter the premises. The button is designed to be easy to find and depress, even in the dark.

The panic buttons used in banks and similar locations are more complicated. The reason is that most police departments will take several actions as soon as they receive the alarm, such as closing down all public transportation systems in the vicinity. Such precautions are very costly and unpopular, of course, and the police departments do not, for obvious reasons, want to resort to them unnecessarily. The panic buttons are therefore designed to be almost impossible to trigger accidentally. They may be either hand- or foot-operated. Usually they must either be activated by using two fingers or by pressing the foot upwards, to minimize the risk of setting them off by accident.

There will also be a discreet indicator installed near the panic button, informing the person activating the alarm that it has indeed been activated. This is usually an LED or a similar light that will remain lit until the alarm is disarmed manually. There must be no question of whether the alarm has been activated or not. There will also generally be a corresponding indicator coupled with a buzzer somewhere in the rear of the office, well out of sight and hearing of the front office where the alarm was set off. This indicator will inform a security officer of the fact that the alarm has been activated. At the same time that the buzzer sounds, the alarm will go to the local police department through an automated dialing system. In addition to this, it is also common for the security officer to verify the alarm by personally telephoning the police.

A personal attack alarm is essentially a wireless panic button. It is designed to be carried on one's person, and, when activated, will trigger the existing alarm system and warning device in the building. Personal attack alarms either rely upon ultrasonic sounds or radio transmissions.

The radio transmitter used as a portable panic button is a fairly obvious design, in effect simply a transmitter capable of activating the alarm system. The transmitter will send a digital code that activates the control unit. The code will tell who activated the alarm but not the location of the trouble. This is a disadvantage, of course. However, the advantage of a radio system of this type is that the range is generally fairly wide. This personal attack alarm can therefore sometimes be relied upon even outside the house.

An ultrasonic personal attack alarm works in a slightly different way. The ultrasonic signal will be received by one of a number of special ultrasonic receivers, one of which is mounted in every room from which an alarm might need to be sent. The ultrasonic signal will activate the receiver, which will in turn trigger the alarm. An LED on the control unit will indicate which receiver triggered the alarm and, consequently, in which room the person who activated it currently is. The identity of the user will not be known, however, if several of these personal attack alarms are in use. Furthermore, the range of this system is much more limited than that of a radio transmitter.

Both these alarm systems can be connected to a personal paging system. The alarm can then be silent, but, for obvious reasons, this is seldom, if ever, the case. If a silent alarm really is desired, then anybody equipped with a personal paging system can be chosen to receive the alarm.

Personal attack alarms should not be confused with the so-called personal alarms sold in many stores. These are small devices designed to emit a painfully loud, high-pitched screeching noise that will surprise an attacker as well as call for help. These alarms are not connected to any alarm system but are sometimes used by people who fear attacks, especially when going out. The efficiency of such an alarm on a deserted street is not very high, however, although it might be sufficient to scare off a mugger.

There are various kinds of personal alarms. Some of them, generally the smallest ones, are activated by compressed air and look like aerosols. Others are powered by batteries or rechargeable power units. Some of them are

activated by a button or a trigger, but they only sound as long as the button is pressed or the trigger is squeezed.

This is especially true of the gas-powered types. More reliable personal alarms work on the principle of a hand grenade. The alarm will continue to sound until it is switched off or the power runs out, even if the alarm is dropped to the ground. This is especially helpful if the situation develops into a fistfight.

Some individuals, especially women afraid of rapists, occasionally wear a whistle instead of any of these types of personal alarms. The idea is the same.

CAR ALARM SYSTEMS

There is a large number of different car alarm systems available on the market today. Some will sound if somebody tries to jimmy open a door or the trunk. Others will be triggered by an attempt to move the car, by towing it away, for instance. Certain alarm systems will even include a remote pager that will signal the owner if his car is being tampered with.

As in ordinary alarm systems, the car alarm includes a control unit, one or more sensors, and a warning device. In a car alarm, however, some of these devices, notably the control unit, will be simpler in design than in the units available for protection of homes and office buildings.

In many cases, the car alarm is at least partially self-contained. No self-contained alarm system is able to protect the entire car, however, including its trunk and hood.

The control unit is often mounted near or on the dashboard, either by using a mounting bracket similar to those used for radios or stereo systems or by mounting it directly to the surface. As the owner generally does not want to give a potential intruder the opportunity to see the control unit, it is often hidden under the dashboard instead, or under a seat, along the firewall, or in the glove compartment. A backup battery is often provided, too, to increase the reliability of the system. Most types of car alarms are operated by either a concealed switch or a key. The sensors used in car alarm sys-

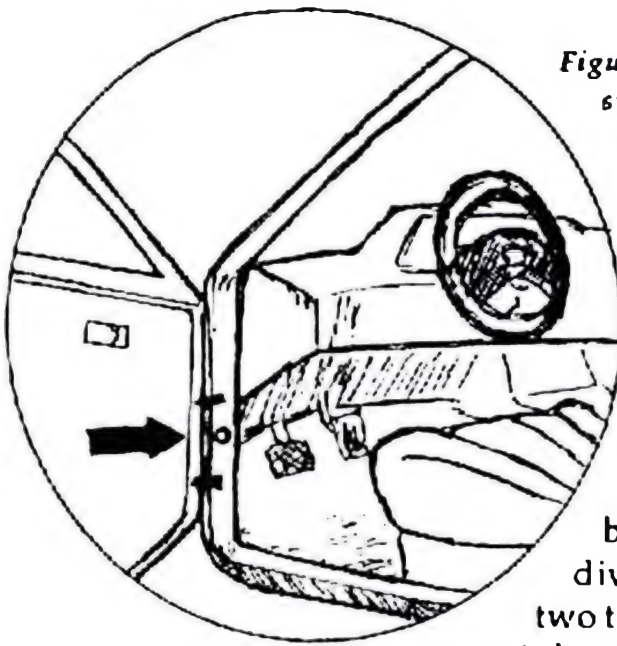


Figure 98. Pin-switch and its location in a car.



tems can be roughly divided into two types: pin-switches that guard

the entry points of the vehicle and motion detectors designed to detect movement of the vehicle.

The most common type of car alarm sensor is the pin-switch (fig. 98), also known as the earth-seeking sensor. This is a door contact switch that is activated when the electrical current is broken. A pin-switch is wired directly to the door and installed in the framing around the doors and/or the trunk and the engine compartment. Pin-switches can also be used to guard the trunk, hood, sunroof, tailgate, or any other point of entry.

Pin-switches are spring-loaded, momentary contact switches similar to the plunger switches described in the previous chapter. The pin is released from the switch when the door is opened, which electrically grounds the system, thus triggering the alarm. This device is linked either to the car horn or to an independent siren. An independent siren is a better option, of course, as it is more difficult to find and disconnect.

As pin-switches have only a single wire connected to them (the car's metal chassis being used as the ground portion of the circuit), they are always installed on a metal surface. When used to protect a door, the pin-switch will be installed near the switch for the interior light on the lower part of the door post.

Some car alarm systems use the switches already installed in the door frames of the car instead of pin-switches. These already installed switches are used to turn on the interior lights whenever the door is opened. Electrically, these switches are identical to pin-switches. In this case, the door frame switches are added to the alarm system by attaching wires to them from the control unit.

The other type of car alarm, very commonly used but not really very reliable, is the motion detector. This is a special vibration switch designed to sound the alarm when the car is shaken or moved. This sensor has a tendency to produce false alarms. Nevertheless, it is very popular. Some control units even incorporate such a sensor in their housing in order to protect the control unit itself as well as the car. Such a self-contained car alarm is difficult to remove without triggering the warning device.

If a motion detector is integrated into the control unit, the unit must always be as level as possible, preferably near the center of the car. If positioned in some other location, it will not be as sensitive to motion at the front or back of the vehicle. The most common location is, once again, under the dashboard.

There are many types of motion detectors. One such type is the pendulum alarm. Such an alarm consists of a pendulum switch and is set off when the car is rocked, jolted, or otherwise moved.

A pendulum switch is used to sense vibration or motion. The switch is designed with a set of contacts that touch each other when it is moved or shaken.

The pendulum itself is a small weight on the end of a light spring with a contact underneath the weight. Whenever something causes the spring to vibrate, the weight will touch the contact and the alarm will sound. The sensitivity of the spring can of, course, be adjusted, but most car owners do not do this. The result is that the pendulum alarm is usually triggered by almost anything, such as the vibration of a passing truck or somebody who happens to bump into the car accidentally. Even a very light jolt is sufficient to trigger this alarm. This propensity for false

alarms has made the pendulum alarm almost totally useless. In neighborhoods where this type of alarm is in widespread use, nobody ever thinks twice about hearing it and there will definitely be no response to it.

A slightly more advanced version of the pendulum alarm is the trembler switch alarm. This device is similar to the pendulum alarm but instead has a ball bearing sitting between two contacts. Any definite movement of the car, such as somebody trying to open a door, will cause the ball bearing to touch the contacts and trigger the alarm.

Both the pendulum and the trembler switch alarms are generally mounted under the hood on the firewall in the engine compartment and can be adjusted for sensitivity. Another common place to find these motion detectors is under the dashboard.

The vibrator contact circuit, or adjustable impact device, is another motion detector. It has a relatively light weight on the end of a piece of spring steel, with a contact under the weight. When the spring steel vibrates, the weight touches the contact, thus activating the alarm. In this device, sensitivity can be controlled by adjusting the distance between the weight and the contact.

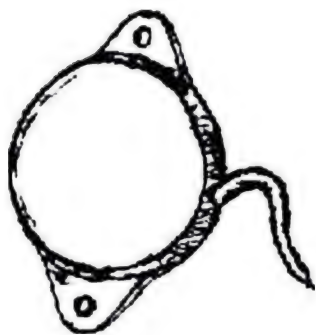


Figure 99. Micro transducer.

Yet another type of motion detector is the micro transducer (fig. 99). A transducer is a device that produces an electric current in response to vibration, shock, or motion. This is a very small sensor, generally round, flat, and like a small coin. This sensor has a small interior piezoelectric crystal that is affected by vibration, very loud noises, or the car being hit by something.

A piezoelectric crystal consists of a crystalline material that will develop a voltage when subjected to mechanical stress or severe vibration and, consequently, produce an electric current that triggers the alarm.

Micro transducers are often located inside the door frame near the switch for the interior light, in the same

position where you would expect to find a pin-switch. Micro transducers, however, can also be found mounted on the center door posts of four-door vehicles. In either case, they are glued in place with epoxy.

Self-contained vibration sensors are also sometimes used. Such a sensor simply consists of a keypad fitted to the dashboard. The alarm, activated by entering a personal code, works like any other motion detector.

Another type of car alarm sensor is the voltage drop sensor, also known as the current-drain sensor. In this device, a sensor is wired into the electrical circuit of the car. Whenever the sensor detects a drop in the voltage, for instance when the dome light comes on as the door is opened or when the key is put in the ignition and the dashboard lights up, the device will trigger the alarm.

This type of alarm can be disconnected, accidentally or not, by the dome light malfunctioning for some reason. It is therefore not very reliable.

More advanced types of alarms are also used as car alarms. Among these are ultrasonic detectors (see Chapter 7). The most common location for such a sensor is usually on the shelf behind the back seat.

A siren is the best choice for a warning device and is in common use nowadays. Various types are available, but they are often mounted under the hood, although well away from sources of extreme heat. The siren is generally mounted slightly downward, as this will prevent excessive accumulation of dirt and moisture. The siren will almost always be connected only to the control unit. Once again, this connection is the vulnerable link in the alarm system. Often the siren will be supplemented by other features, such as a light-flashing facility. Such a device can easily be wired into any of the numerous types of alarm systems.

Finally, remote sensor alarms can be fitted to roof racks and trailers. The really security-conscious can combine all of these options in the same alarm system.

Other specialized features of car alarms include the so-called "passive" alarm system, which automatically arms itself once the owner has locked the car. This alarm is usual-

ly armed and disarmed by means of a concealed switch inside the car. Therefore, a certain delay is imposed before the alarm is sounded so that the owner will have enough time to open the vehicle and disconnect the system. Other alarm systems are manually armed and disarmed with an external security key switch, usually located at the rear of the vehicle.

A variant of this system relies instead on an infrared transmitter kept on the owner's key ring or on any other hand-held device. After stepping out of the car, the owner simply aims the device toward the receiver mounted inside the car and presses a button. The infrared beam will activate the system. This will lock all doors and set the alarm. In some versions of this alarm system, the car will even flash its headlights to indicate that the message was received and understood. The alarm can be switched off and the doors unlocked in the same way. Another variant of the same idea is the key ring containing a small radio transmitter that emits a radio signal. Locks of this type are generally called remote control locks.

Another interesting option on many control units is a built-in radio transceiver (a receiver with transmitter). This device will allow the alarm system to be armed and disarmed, or even tripped, by a miniature radio transmitter built into a small pager unit. This circuit will alert the owner to the fact that his car is being tampered with.

Remote paging car alarm systems of this type are especially popular in areas where there is little likelihood of somebody else noticing the alarm if it is sounded. The owner, who carries a remote paging receiver to alert him whenever the alarm is sounded, is then free to investigate himself, call the police, or both.

These systems are sometimes used as silent alarms, without an ordinary siren, especially if the owner hopes to catch the intruder in the act. Some alarms of this type allow the user to choose between siren and silent alarm operation. Those remote paging systems that can arm or disarm the alarm system from a distance almost invariably include a panic button as well with which the owner can activate

the car's siren if threatened or surprised by intruders. This option is popular among people who fear walking alone through empty parking lots and professional truck drivers who might have to stay around their vehicles for long periods and even sleep in them frequently.

The remote paging system consists of two parts. The combined transmitter and control unit is mounted in the car, powered by the vehicle's electrical system, while the battery-powered remote paging receiver is small enough to keep in one's pocket. Although these two devices work on a radio channel that is on a frequency seldom used by most radios, they will also be safeguarded by a security code that is always sent when the transmitter is triggered. This will prevent accidental triggering and is also supposed to prevent an intruder from using his own transmitter to disarm the alarm system. The latter is not valid, of course, as an intruder can easily determine and imitate this code if he has access to specialized equipment. (Such equipment is costly, however.)

When the transmitter is triggered, it will send out a signal containing the security code. The paging unit, when detecting a signal on its preset frequency with the proper code, will start beeping. It generally also flashes an LED. The security code is selected in advance by setting a group of internal dip switches. These switches can naturally be found in both devices.

The transmitter will use the vehicle's standard antenna, including the type that automatically rises when the radio is switched on. The intruder can therefore prevent the antenna from rising, which will decrease the range of the transmission severely. The vehicle might of course also have a wire-type antenna built into the windshield, but then the effective range of the transmitter will be significantly reduced in any case. Some vehicle owners attempt to extend the range of the transmitter by installing a separate antenna. Remember, though, that the transmission in this alarm system is the same as the wiring in ordinary alarm systems and should therefore be cut by an intruder. If the alarm call transmission can

be prevented, the owner will not be alerted.

Generally, though, the transmission will be sent. The range is then completely dependent on the terrain and the characteristics of the surrounding area. The range might be several kilometers in open country or be reduced to a few hundred meters or less in a city or an underground parking lot. The strength of radio transmissions will also often be reduced considerably by the metal used in most high-rise buildings. Most alarm systems manufacturers claim an "average" range of 3 kilometers, but this is quite an exaggeration. Between 200 and 500 meters is a more typical range within a city. In fact, the transmission can be eliminated by enclosing the transmitter in a metal box. Were it not for the antenna and, to a lesser degree, the windows, the car is, in effect, such a box.

Many car alarms are modified for use in other vehicles and locations, such as boats, trailers, campers, etc. The remote paging systems are especially popular, as they have a great range (more so if connected to a citizen's band base station antenna) and are therefore sometimes used to guard scattered buildings or stores on farms and construction sites.

The car alarm is otherwise armed and disarmed using several different methods, depending on whether a delay is built into the system or not. If so, the delay might be as short as twelve seconds or as long as forty seconds or more. Arming can, for instance, be done by turning the ignition key switch to the ON or ACC (accessory) position for a few seconds and then switching it to OFF. This will arm the alarm system after an exit delay period. It is then disarmed by simply entering the car and switching the ignition key switch to ON before the entry delay period is up.

Another method of arming and disarming is by a switch on the control unit. The easiest, of course, is when the process is performed automatically whenever the ignition is switched on or off. In many cases, the control unit will inform the user of the fact that it is armed or disarmed by either producing a beep or lighting an LED. Sometimes a combination of the two is used and sometimes neither is used.

A valet switch might also be present. This is a switch

that allows the owner to bypass the alarm system when he expects to be away from his car but knows it will be attended or guarded by valet parking or servicing, for instance. The valet switch can only be activated while the engine is running and is therefore of little use to an intruder.

Many car alarms are powered by the car's own battery, but it is also quite possible to add a second power unit as a backup. This is mainly done in commercial vehicles, as on many of these it is easy to gain access to the battery terminals and then disconnect the ordinary alarm. Remember that it might be possible to disconnect the wiring from underneath, even if the battery is locked away under the hood. Having a backup power facility is therefore always prudent.

Almost all car alarm systems are designed to be powered by 12-volt DC current. Furthermore, the wiring is often easy to identify, as a color-coding scheme is common in many countries. For instance, red wiring is used to connect the system to the power source, the car battery. Other colors might be used to identify the components of other systems. Remember, though, that this often varies in different countries—and even in alarm systems manufactured by different companies in the same country.

A professional car alarm system will also have closed circuit wiring. This means that the alarm will sound even if the wires to the sensors are cut. However, the system still will not work if the wire to the warning device is cut instead.

Sometimes the purpose of the entry operation is not only to break into a vehicle but also to move the vehicle in question. This leads to several other considerations, apart from the lock and alarm system.

If the car must be moved, remember that the vehicle might have been immobilized in some way. There are several ways of immobilizing a car. Both electrical and mechanical methods of immobilization can be used, and they should be prepared for.

The electrical means of immobilization include fitting one or more devices, such as an ignition cutout device, to the car. This can be a part of the vehicular alarm system and is then either linked to the car's horn or to any other siren.

The device will sound a warning at the same time as it is blocking the ignition circuit, automatically immobilizing the car.

A manual ignition cutout device is also useful. An ignition disabler switch can be hidden under the dashboard, for instance, and will interrupt the ignition feed wire. Note that the car can still be hot-wired and started easily if the interruption is made between the battery and the coil. If the interruption is made between the coil and the distributor, however, this is not generally possible. The switch might require the use of a key to open.

A passively armed cutout device will render the ignition dead as soon as it is switched off. When the driver wants to start the car again he must deactivate the cutout by depressing a button or switch while he starts the engine.

Yet another method is to use a removable circuit card. Usually this card is put into a socket mounted on the dashboard. When the card is removed, however, vital electrical circuits will be broken, preventing the car from starting. Another method of electrical immobilization is to fit a switch that interrupts the feed wire to the electric fuel pump.

A multiple cutout device can also be incorporated into the central control unit. The unit is bolted to the bulkhead under the hood and disrupts several electrical circuits at the same time. Finally, the vehicle can be immobilized by simply swapping or removing a couple of the spark plug leads.

Mechanical immobilization methods include the use of an engine immobilizer switch, the previously mentioned hidden switch in the ignition circuit, or an internal locking device that is, for instance, fitted over the handbrake and locked around the gear lever. Locks that are simpler, but also fairly reliable, include combination locks attached to the handbrake, engaged or disengaged by means of a three-digit combination. Such locks slide over the top of the handbrake lever, locking it in the "on" position. Electronic locks that prevent the engine from starting until the driver has entered the correct code on a keypad fixed to the dashboard can also be procured.

Additional steering wheel locks are also commercially

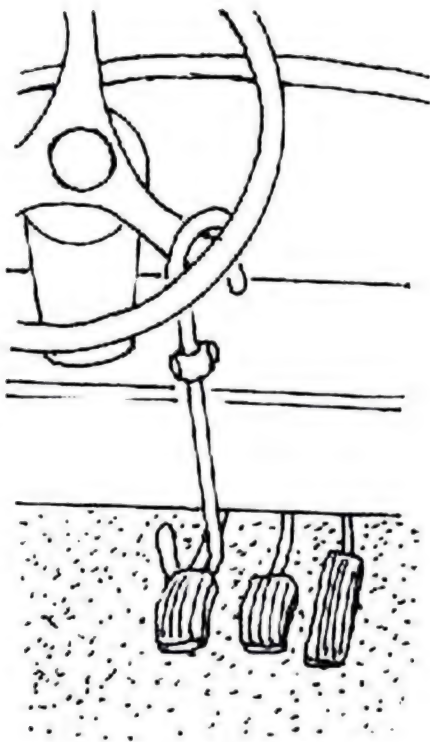


Figure 100. Steering wheel hook lock.

available, although they often are of the hook type, hooking on or over the steering wheel and brake, accelerator, clutch pedal (fig. 100), or floor-mounted gear stick. If the device is hooked over the clutch pedal, an intruder can easily get rid of this device in an emergency by simply stamping down hard on the clutch. As the steering wheel bends quite easily, the lock will come off. If the brake pedal is used instead of the clutch pedal, however, this procedure is sometimes more difficult to perform. Of course, the quality of the locking device will also affect the outcome.

Additional locks can be fitted around the steering column like an armored collar. The lock key will then replace the vehicle ignition key and control the electrical operations. Although good in principle, this can easily be demolished with the use of heavy-duty tools.

Some suspicious individuals remove the rotor arm from the distributor in order to protect their cars from theft. The distributor cap is easy and quick to snap off in order to remove the T-shaped rotor arm sitting in the middle of the distributor. It is small enough to put in a handbag or pocket. Others remove it and then lock it in the trunk.

A final, and very definite, method of mechanical immobilization is to use a wheel clamp, also known as a Denver boot. This will effectively prevent the car from being moved. Most wheel clamps also prevent the tire and wheel from being removed. These can be found on cars that are left unattended for considerable periods of

time or have been secured by the police.

Vans, trailers, and motorcycles present still other problems, especially if they must be moved from the location in which they are found.

Vans and trailers are sometimes safeguarded from towing by locking a hitch lock, or tow ball, into the ball socket of the vehicle-towing hitch. Such a device can only be removed by using the correct key bar. The lock must be picked or else broken.

Motorcycles and bicycles are generally secured with chain locks. These are generally easy to cut through with bolt-cutters, especially if they are not of made of hardened steel. For this reason, specially designed padlocks with hardened, elongated shackles are often used instead. The steering lock of a motorcycle is usually of simple construction and can often be broken by a fierce wrench of the handlebars. Although motorcycles can be fitted with electrical immobilization devices and alarm systems, this is very uncommon.

It is more common to immobilize the motorcycle by removing the battery ground strap or the line fuse in the main lead near the battery terminals. A concealed cutout switch that breaks any of the low-tension wires to the coil can also be fitted. As long as the correct equipment is available, neither of these methods will present any problems to the operative.

Other measures used to protect a motorcycle for long periods of time include such devious alterations as fitting unserviceable but visibly complete spark plugs, draining the float chambers and removing or blocking the fuel supply line, or putting the bike in first gear and then removing the gear and clutch levers. Once again, should it really be necessary to move the motorcycle, this is only a matter of having the correct spares available.

SHOPLIFTER DETECTION SYSTEMS

Alarm systems designed to detect and scare away shoplifters have been in widespread use for a long time.

Several types exist, and all of them are still very common.

These types of detection systems rely upon fastening some kind of indicator or tag to each object to be protected. In an electromagnetic system, the tag might be a magnetic tape, for instance, while in a radio frequency system, it will be a special coil on a circuit card. In either case, the alarm will sound if the tag is passed near a specially designed detector.

The radio frequency system is easiest to use, as the electromagnetic detectors are very clumsy. However, the radio tags are always active, which might cause complications. The radio frequency system will also sometimes trigger a false alarm if exposed to portable radios. Furthermore, the tag can be rendered inoperative by being hidden in a metallic cover. This will nullify the signal and prevent the alarm from sounding. For these reasons, neither of these systems is very popular.

The British company Securitag International is currently the major manufacturer of shoplifter detection systems. Its products are very popular, as they rely on a completely different technique.

The Securitag system also consists of tags that are affixed to the goods to be protected; however, the actual functioning of the tag is different. The detector posts continuously send out a low-frequency signal that will trigger any tag that is brought within range. The activated tag will then respond by transmitting another signal. This signal will trigger the alarm.

Whenever a tag is brought out through the door, it will transmit a

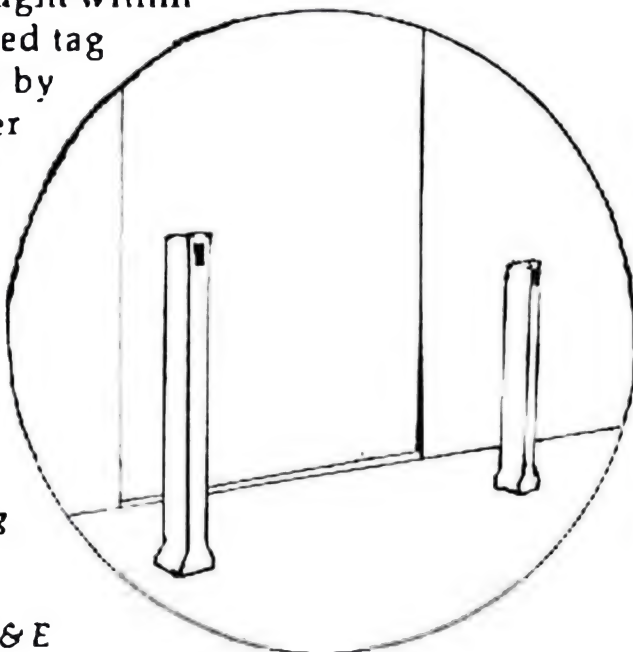


Figure 101. The Securitag system.

signal that is received by the detector posts positioned either near or on either side of the door (fig. 101). Every detector post has a range of about 90 centimeters. Alternatively, a detector loop can be installed around the door, in which case no posts are required.

Because of the design of this system, there is no chance of a false alarm being caused by portable radios or metal objects.

The tags are naturally extremely difficult to remove without the special equipment available from Securitag. However, as this equipment is the same in all Securitag units, an intruder can generally acquire it easily should it ever become necessary.

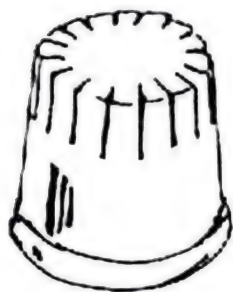
As a curiosity, it should be mentioned that this idea was originally introduced by the KGB for use in electronic surveillance operations.

FIRE ALARM SYSTEMS

Fire alarm systems are sometimes combined with intruder alarm systems, but the two are more often separate. The warning sound used in fire alarm systems is usually distinctly different from that of intruder alarm systems. This is generally true whether the systems are connected or not, except in the simplest alarm systems.

Whether the fire alarm is incorporated in another alarm system or completely self-contained, it will more often than not rely upon either one or both of two radically different types of sensors. These are the smoke detector and the thermal detector, both of which are very common. Yet another type of sensor, the differential detector, is also used sometimes.

The smoke detector (fig. 102) is placed on the ceiling or high up on a wall, as smoke always rises. Several smoke detectors, either self-contained or alternatively connected in parallel, can often be seen in bedrooms or at least in a common hallway.



There are two different kinds of

Figure 102. Smoke detector.

smoke detectors, the ionization type and the photodiode (or photoelectric) type. They differ in the way they detect the smoke that will trigger the alarm. The ionization type is most popular.

An ionization smoke alarm has a small internal chamber containing a very small amount of radioactive material. The air in the small chamber is ionized and therefore able to conduct an electrical current. Since the radioactive material is located between two electrically charged electrodes, the ionized air will conduct the electrical current between them. If smoke particles (excess carbon particles in the air) enter the chamber, they will increase the resistance of the ionized air. This will naturally decrease the flow of current between the two electrodes. The alarm will sound when the resistance has increased to, and the current flow drops below, a certain preset point. This happens whenever there are too many carbon particles in the air.

The photodiode smoke detector relies upon a beam of light that is projected across a sensing chamber onto a photoelectric cell. When smoke particles enter this sensing area, the light beam is disturbed and the level of light reaching the photoelectric cell is reduced. The alarm is triggered when the level of light reaching the photoelectric cell drops too much.

The reason ionization alarms are the most popular is that they will respond slightly faster to a rapidly spreading fire. Such a fire always produces many smoke particles. Both types are reliable, however. They will even respond to the tiny smoke particles produced by a fire before actual smoke can be seen.

Sometimes a high level of dust in the air will produce a false alarm when it accumulates inside the sensor. Dust in the sensing chamber might also reduce the sensitivity of the alarm. Other sources of false alarms might include small insects or high humidity.

Self-contained smoke detectors have integral batteries, usually of the carbon-zinc or alkaline types. Alkaline batteries are the most reliable, as they last longer. Despite this, they should be checked at least once a week for safety reasons.

Although a reset button is included in the alarm, the continued presence of smoke will simply result in the sounding of the alarm again. Therefore, it cannot simply be turned off as long as the conditions that triggered it remain.

Smoke detectors can generally be used in any room except the kitchen. Thermal, or heat-sensitive, detectors are used there instead.

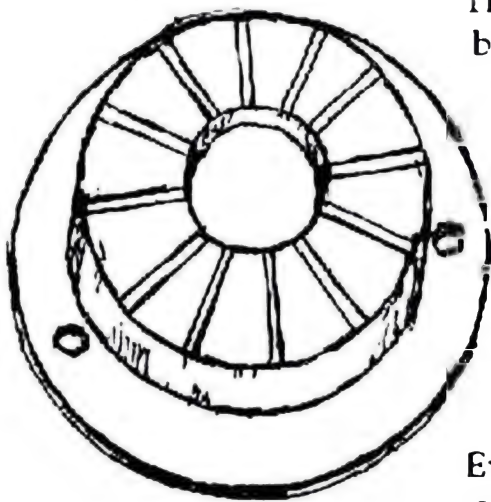


Figure 103. Thermal detector.

Thermal detectors (fig. 103) use built-in pyroelectric sensors able to sense when the temperature in the room rises above a dangerous level. The exact temperature level that is deemed critical depends on the construction of the sensor.

Typically, though, 50°C is the most common in Europe, while 135°F sensors are used in the United States, except in kitchens and furnace areas where a higher temperature is normal. In these areas, 80°C or 190°F sensors are used instead. The sensor contains a material that will melt at the chosen threshold temperature. This will produce electric contact and trigger the alarm.

Thermal sensors can also be wired in parallel. Except in kitchens, they are used mainly in areas where fires that produce more heat than smoke—certain types of electrical and chemical fires, for instance—are likely to occur. Yet another type is the differential detector. This is an advanced thermal detector for use in environments that are unsuitable for ordinary detectors, such as certain kitchens and garages. This detector works by adapting itself to the temperature in the area. It will trigger the alarm when the temperature rises more than 5 degrees per minute.

For a professional intruder, the main advantage of a fire alarm system that is part of an intruder alarm system is the fact that the fire alarm will override the actual intruder

alarm. This is very useful, as the deliberate activation of the fire alarm might provide an easy diversion. It is not really necessary to start a fire in order to activate this type of system. Simply blowing smoke into a smoke detector will trigger the alarm. Afterward, there will be no explanation as to why the fire alarm sounded at that particular time. The operative might even go to the trouble of blowing some dust into the detector in order to make it appear as if the alarm malfunctioned.

The fire alarm is easy to find if present. As smoke will to some extent be impeded by doors, most fire departments recommend the installation of several sensors, optimally one in every room. There will be at least one in each hallway, however, and probably one in the kitchen or in other areas where a fire is more likely to break out, such as near heating units and fuse boxes. They are almost invariably mounted on the ceiling, generally at the center of the area they are protecting.

Entry Tricks

This final chapter will be devoted to several of those tricks of the trade that one day might be useful to the field operative who is involved in entry operations. These tricks include ways of finding plans of the target's alarm system, as well as recognizing traps and faked obstacles to the operation. Common hiding places of keys and combination codes also fall under this heading. All these methods help the operative avoid capture when on an entry mission. Every additional advantage increases the security of the operation.

The easiest way to enter the residence of an unsuspecting owner is to use the real keys. If the owner leaves the keys outside his house when he goes away, this is quite easy. The operative should therefore check the seven most common hiding places for keys:

1. under the doormat
2. under a flowerpot
3. in a flowerpot
4. under a stone alongside the path or near the front door
5. stuck or hanging under the window ledge
6. hanging inside the door on a piece of string that can be pulled through the letter box in the front door
7. just inside an unlocked garage or storage shed

If the operative can gain entrance to the house for a few moments, he might be able to check whether the key is left in the lock on the inside or in an obvious cupboard or hook near the front door. If so, he might get an unsupervised moment in which to make a pattern of the key in a wax box. Then he can make a copy at his leisure.

Sometimes supposedly locked doors are nevertheless found unlocked or even opened. The reason is usually very simple—there is work being done on the premises which is facilitated in this way, for instance, or a visitor or delayed employee is expected to arrive shortly. Some people regularly leave the door unlocked, especially in offices, so that they do not need to use the key when they return. But the human factor is not always the reason. The lock may be installed incorrectly, so that the door will not lock even when closed, or the door check does not work properly.

For this reason, many companies employ a guard or a caretaker to regularly check that all doors are locked and remain so. If the guard follows a fixed routine, however, you can plan the operation so that he is safely out of the way. Otherwise it is a good precaution to position a colleague to watch out for the guard so that you know when he is making the rounds.

The points of entry include, but are not limited to, doors, windows, and any other openings that provide access to the interior of the target building. As was mentioned in Chapter 6, it is also sometimes desirable to enter through a roof or ceiling. Most houses protected by an alarm system have a sensor on each outside door or window that is accessible from the ground and large enough to crawl through. Windows on the second floor are generally not protected, however, unless they are easily accessible from a flat garage roof or a tree. If they are accessible, but not easily so, and at the same time cannot be seen from the street or from a neighboring house, they might be protected by alarm sensors. Try to pinpoint the sensors before the actual entry attempt. There might be an opening that has been overlooked.

As every burglar knows, whether he is a criminal or employed by his government, there are certain indications

of whether or not a house is empty. One of these, maybe the most important, is the absence or presence of light.

Many houses today are equipped with outside lights that are switched on at dusk every night by a light-sensitive photoelectric cell controller. Such a device measures the intensity of natural light. It will be triggered by the natural light levels and switch on the light, when the light falls below a certain, predetermined level. The lights will be switched off automatically when daylight returns. Other buildings rely on programmable automatic timer switches that regularly turn on the light at a predetermined time.

Some of these timer switches are of the twenty-four-hour variety that will turn the light on and off at the same time every day. Others are the seven-day type that can be set to turn the light on and off at different times each day of the week. The switching pattern will be repeated only after a week has passed. Sometimes the users of these devices even realize that they must vary the setting of the timer with the changing of the seasons. There are devices available for this very purpose. They can be programmed to vary the times the light, or lights, will be turned on each day, according to the seasonal changes in the day's length. These devices are called solar dial timer switches.

Such devices are often both powered by and transmit their signals over the electrical wiring in the building, although remotely controlled units utilizing radio waves are also available. The lighting may even be connected to the output from the alarm system, so that all or at least most lamps in the building will turn on or start to flash whenever the alarm sounds. Other appliances, such as stereo systems, can also be activated in this way. Virtually nothing is impossible, but the sobering fact remains that this will not prevent a professional intruder.

Finally, passive infrared detectors might be used for turning on the light as soon as somebody approaches. Such a detector is easily wired to a light source, and the light will remain on as long as there is somebody in the vicinity emitting body heat or for a set period of time after the source of warmth has gone. Such an infrared floodlight system

includes a built-in photoelectric cell that prevents it from triggering during daytime. Sound-triggered detectors are also available for the same purpose.

Another security device is an electric curtain controller, which will open and close corded curtain sets. This device is generally connected to a timer for automatic control.

A radio, preferably tuned to a "talk" station, is often left on or turned on with a timer switch as well. Finally, a telephone answering machine programmed with the message that the owner "cannot get to the phone right now" (not "I'm out") is also frequently used to leave some doubt as to whether anybody is at home or not.

However, these means of scaring away ordinary burglars are not very effective. It is generally easy to check whether anybody is at home or not, by making a personal call pretending to be a salesman for instance. Furthermore, some people leave the light on only in the hallways rather than in the living rooms. This is a definite indication that the house is empty, as nobody actually lives in the hall. Leaving the light on in a downstairs room with the curtains closed it is slightly more clever, but not enough so to deter a professional intruder. Most individuals who use this ruse to protect themselves are instead advised to leave the light on in an upstairs bedroom, where an intruder cannot peer in to check whether it is occupied or not.

It should also be mentioned that cutting the electrical power and /or the telephone lines will effectively determine whether anybody is at home or not, as the owner is certain to reveal himself if he really is at home. Furthermore, it will render useless most of the previously mentioned protective light systems, etc.

Therefore, some people instead use a recording of a barking dog, which is activated whenever a doorbell is depressed. There is even a self-contained alarm system available that will imitate the sound of a dog whenever somebody is approaching the protected area and is detected electronically by a passive infrared detector. These various dog imitation systems can always be identified by the fact that you will only hear the actual barking and no other noise such as the

dog running around or jumping at the door.

On the other hand, real dogs are a very serious problem, especially if they bark at strangers and generally appear unfriendly. Guard dogs are not always dangerous, as they are mainly kept as a psychological deterrent to frighten intruders away rather than actually attacking them. Terriers, for instance, make excellent guard dogs for this reason. But whether the dog is really dangerous or not, its bark will call unwanted attention to the scene, so dogs should always be avoided, or at least silenced in some way, if at all possible.

Certain large dogs, such as the Great Dane, the mastiff, the Alsatian or German shepherd, the Doberman, and the rottweiler, are sometimes trained not only to set off the alarm, but also to defend the home against attack. Really dangerous patrol dogs are not usually kept as domestic watchdogs, however, as they are simply too dangerous unless in the care of a professional dog handler. Here, too, it is important to avoid the dog by all possible means.

As a curiosity, it might be noted that in rural areas, geese present a very real obstacle. Geese are highly territorial, and not only do they honk furiously, they also often chase and peck any intruder who does not retreat quickly enough.

Many apartment complexes employ audio entry systems. This is a means of access control in which a speaker panel is located outside the premises near the front door. The speaker is linked to a telephone handset or microphone device that permits two-way speech. The device is frequently used in conjunction with a digital code lock entry system. Each flat in the building is then equipped with a telephone handset as well as a remote control that releases the electrically operated door lock.

The audio entry system might also include an audio-visual component. It will then function as the standard audio entry system but with the addition of closed circuit television (CCTV).

It is, however, easy to circumvent an audio entry system. Just call up anybody in the building and either say that you have lost the code but a "friend" (who you know is a

resident in the building and whose name you will mention) asked you to go inside and take care of something in his apartment. If this does not work, call up another one and say that you will have to enter to deliver something (not the mail, though, as the postman will have the correct code and does not need to ask for it). If all else fails, you can always say you want to come inside to deliver free samples of something you believe is desirable to all of the tenants in the complex. Of course, it might also suffice to wait for somebody to arrive and then enter with him or her.

There are also certain popular ways to gain entrance to a private home, during the preliminary reconnaissance of the premises, for instance. Such methods are frequently used by con men. The operative dresses up as an official, a salesman, or in any other suitable disguise. Then he approaches the target.

He might claim to be from the electricity, gas, or water board, for instance. The "electricity board representative" can ask the owner of the house to stand by the fuse box and turn the power on and off while he goes around the house to "check the circuit." The "gas board representative" might ask the owner to watch the meter outside while he "checks the appliances." The "water board representative" might ask the owner to turn the taps in the kitchen while he "checks the flow" in the other parts of the house, such as the bathrooms.

All of these disguises do carry the risk of the owner of the apartment asking for an official identity card, first of all, and then locking himself in his apartment while calling the local office to ask them about you. You can sometimes avoid this by having the telephone number of a colleague printed on your (faked) identity card. However, this sometimes backfires, too, as the real government office will be listed in the telephone directory.

In the early 1980s, a foreign operative who was working under embassy cover in the former Soviet Union planned to enter the dacha, or country villa, of a local party official. The plan was to enter in order to plant electronic bugs in the building. The party official himself was not very important,

but his brother was a high-ranking member of the KGB. It was assumed that one could pick up interesting gossip on the occasions when the KGB brother visited the house.

In order to have a first look around, the operative dressed up as an official. He made a personal call to the family in order to make inquiries about the rating of the house. Such inspections were fairly common there, although less so when it came to influential party officials.

The brother of the KGB officer was unexpectedly cooperative, however, and during their conversation, the operative realized that the official had actually asked for a rating to take place. The reason was that his dacha was not big enough. Now he was overjoyed, as he expected the operative to help him find a bigger one.

What was worse, it soon turned out that the real rating official was expected to arrive later the same day. At this point, the foreign operative hurriedly excused himself and left. The operation was abandoned, and the official's house remained free of electronic bugs.

Despite these and other obvious risks, it is amazing how easily most individuals are taken in by such simple tricks. It is always worth a try, as long as an escape route is prepared in advance.

The operative might also disguise himself as a salesman. Then he might offer a free estimate for carpets, furniture, or anything else that will be so attractive in price that it will enable him to enter the premises. A variant of this theme, in rural areas only, is the itinerant antiques buyer who wants to browse around the house looking for interesting pieces to buy.

In rural areas, where open solid fuel fires are common, the field operative can choose to disguise himself as a chimney sweep. A common trick used to be left alone in the house is to tell the owner to go out into the garden and shout when he sees the brush coming out of the chimney.

It is a great advantage to know in advance of the existence and type of any alarm or locking device in the building. In some countries, notably the United States, many cities and counties require a permit for installing an alarm

system. Therefore, the relevant archive might be a good source of information regarding the possible existence of any such means of protection.

The plans for an alarm system will often be kept at the security company that originally designed it. The installation codes and operator codes will also be kept there. If you can gain entrance to this company's office, you can take advantage of this information.

Finally, it must be remembered that the local fire prevention unit will have a say when a major alarm and lock system is designed. This might mean that the fire station will have a copy of the plans, including master keys in certain cases. It might also mean that some exits will be left open, or almost open, on purpose, regardless of the risk of an intruder entering. The safety of the personnel working on the premises is generally a higher priority than the ability to keep intruders out. This is especially important in a building where burglars are not expected to be interested in the merchandise or machinery.

Vehicles are nowadays protected in many different ways. In some cars, for instance, the standard locks will have been replaced by new ones. Still, all too many people frequently lose their car keys. For this reason, some cars have a magnetic box containing a spare key that fits under the car. If you find such a box, entry into the car is very easy, of course. Just open the box and retrieve the key.

***THE
RIP-OFF
BOOK***

***VICTOR
SANTORO***

Contents

Introduction	1
A Short Glossary of Terms	3
What is Fraud, Anyway?	4
Why Frauds?	7
Myths About Frauds and Victims	9
Crime Pays	12
Why are We Vulnerable?	16
Portrait of the Fraud Artist	21
Anatomy of a Fraud	23
One Step Ahead of the Law	26
Classic Swindles	28
Advertising Frauds	42
Business Frauds	44
Chain Letters and Pyramids	48
Door to Door	49
Drug "Burns"	54
Entrapment	56
Fleeing Relatives	60
Gambling Dangers	63
Health Care Fraud	66
Income Opportunity and Job Offer Frauds	80
Insurance	87
Intentional Accidents	89
International Frauds	91
Money Swindles	94

Moving Goods	99
Personal Deceptions	102
Personal Improvement	106
Personal Property	110
Playing on Hopes	113
Postal Frauds	115
Real Estate Frauds	124
Stock Market Frauds	132
Tangential Cons	136
Technological Fraud	139
Telephone Games	142
Third-Party Contracts	146
Striking Back is Healthy	148
Passive Defense	150
The Role of the Police	154
Active Defense	158
The Principles of Counter-Attacks	163
Counter-Attacking Through the Mails	166
Putting the Heat on the Boiler Room	169
Cramping His Style	173
Inside Work	177
Direct Action	180
Impersonation	182
Planted Evidence	186
Long-Range Techniques	188

INTRODUCTION

The purpose of this book is to outline the basic principles of fraud and specific techniques fraud artists use to milk the public. The reader will learn to protect himself against many types of fraud by understanding the ways in which con men work. He'll also learn to protect his interests in transactions which fall into a gray area. These are transactions which, although not fraudulent in the eyes of the law, are yet shady and filled with danger for the innocent consumer.

We shall see that there is no clear dividing line between honest deals and frauds, and that there is an element of deception in many transactions.

The scope of this book will be limited, giving certain areas little or no attention. Gambling, for example, is a lucrative field for cheats, and most people should be aware that there is a risk of being defrauded when they gamble. It seems unnecessary to pound very hard upon this point.

Sophisticated white-collar crimes, such as embezzlement, bribery and kickbacks, will get no attention because victims are corporations, the officers of which are well-versed in the means of protection and detection. Employee thefts of various sorts, from physically stealing goods to faking expense account vouchers, affect ordinary citizens in that they can result in higher prices, but will not be covered because there is nothing the consumer can do about them.

The focus of this book will be on frauds aimed at working people and small businessmen, concentrating on the principles and techniques involved. The reader will learn how to forestall fraud by recognizing the methods and avoiding the traps. In this regard, there will be much discussion of borderline areas, not legally defined as fraud, and we shall see that there are many deceptive practices used without infringing the law because the law seems to be one step behind the clever fraud artist.

There will be outlines of methods by which the consumer can protect himself, both passively and actively. Finally, unlike most

consumer-oriented publications, this one contains explanations of the means of overt counter-attack against fraud artists, in an effort to help the reader understand that he or she does not have to be a passive and helpless victim because of the impotence of law-enforcement agencies.

A SHORT GLOSSARY OF TERMS

CON, CON MAN, CON GAME. This comes from the word "confidence," and originally was used in the sense that the fraud artist operated by gaining the victim's confidence.

MAIL DROP. An accommodation address which permits the fraud artist to receive mail at other than where he lives. While the Postal Service offers patrons mail boxes, it requires that the renter of a mail box provide his correct name and address. It is a crime to rent a post office box under an assumed name. Postal inspectors monitor closely the traffic to P.O. boxes and are alert to their use for fraud. Private operators, on the other hand, need observe no such restrictive regulations, and they rent their addresses to anyone who puts up the money. Their customers often have furtive purposes, but not necessarily criminal ones. Those seeking sexual contacts, for example, who write to "swinger's" clubs, often do not give their home addresses, either because they lead secret lives and do not want their families to know, or because they want to screen their mail without letting the writers know where they can be reached. Also known as "letter drop," "mail forwarding service," and "remailer."

MARK, JOHN, PATSY, PIGEON, SUCKER, are all synonyms for victims.

PENCIL. A front man in the operation of a dubious enterprise. The Pencil is often a legitimate accountant or lawyer, who does not know the real nature of the business. The Pencil is often used in the more elaborate fraud schemes, such as taking over and milking a legitimate business, not in what we call consumer fraud.

SHILL. A confederate or collaborator of the fraud artist. A shill will often pose as a customer at an "auction," bidding up the price and leading the suckers on. He will also serve as a third party in a gambling scheme, a "pigeon drop," or a "Murphy" game. Also known as a "Steerer."

WHAT IS FRAUD, ANYWAY?

In attempting to define “fraud,” we’ll gain an insight into why fraud artists are so hard to stop and prosecute. The same problems we have in defining it trouble legislators and police, and make arrest and prosecution very difficult.

Most of us know what we mean by fraud. We can say that fraud is an act to take money or other valuables from another person, for profit, and by means of deception. That’s a simple definition, avoiding fancy words and legal terms.

Let’s break down that definition and examine each part:

Taking money from another is often legal, when there is an honest transaction, such as working for it, or selling an honest product.

There’s nothing wrong with making a profit, as everyone who works for a living faces the problem of selling his time or product for a profit. However, the question of how much profit is legal or legitimate is one that concerns lawmakers very much. Every several years, for example, the media present stories of defense contractors charging the Government extraordinarily high prices for simple items available at a supermarket or hardware store for a tiny fraction of the price. Selling a bolt or a pair of pliers for hundreds of dollars certainly appears illegitimate, although a prosecution for fraud is unlikely.

Deception is the key to fraud, and the hardest element to prove. Except in the case of a well-known or well-established fraud scheme, such as check kiting, it is very difficult to prove that there is intent to defraud.

Let’s look at a few examples to see how hard it is to prove fraud exists:

Many people look for “investment” items they can buy in the expectation of either returns on their money, such as dividends, or being able to sell at a profit later on. When a seller offers a piece of real estate, and suggests that it will go up in price in years to come, it could be an honest transaction or it could be a fraud, depending

on whether the seller knows the real estate is worthless and has no hope of appreciating. Proving what is in his mind is the hard part.

When a doctor advises a patient to have unneeded surgery or other treatment, he could be seeking to line his pockets, or he could be making an honest mistake. This, too, is very hard to prove, and very few doctors lose their licenses over this issue and almost none are prosecuted, although the amount of unnecessary surgery and treatment in this country is appallingly high.

In many cases, the seller is promoting something intangible, such as happiness. "Lonely hearts clubs," for example, are selling the prospect of a romantic relationship, and the situation is such that they cannot control whether or not two people so introduced will be able to establish a long-term relationship. This, too, makes prosecution very difficult.

When a seller offers goods or services and the buyer is disappointed, it might be fraud, or it might be an honest disagreement over the terms of the sale or the nature of the product or service. In many instances, it is a matter for civil litigation, not criminal prosecution.

For example, there are many fly-by-night home improvement rackets, but a contractor who sells a home improvement or repair that is defective is not necessarily a fraud artist. His firm may simply do sloppy work. In deciding whether or not to prosecute for fraud, the police must take into account the fact that the dividing line between fraud and legitimate business is so thin as to be invisible, and they will investigate to determine whether the accused is a long-established businessman who warrants his work and whether the majority of his customers are satisfied.

This theme will recur throughout this book. There are many businesses that operate on the thin edge of the law. Distinguishing between a legitimate one and a fraud operation is often impossible, partly because of inadequacies in the legal definition of fraud, and partly because frauds and legitimate enterprises resemble each other so closely, and often engage in the same tactics. In many instances, we must conclude that a business is not an outright, prosecutable fraud, but yet is "shady." Prominent examples of

these are marriage counselors, sex clinics, weight loss and smoking clinics, and various “alternative health care” practitioners.

Unfortunately, the size and longevity of the business are not a reliable guide. In the examples cited above, of defense contractors overcharging the Government, the companies involved are among the largest in the country, and in the well-known electrical industries price-fixing case of the early 1960’s, the names included such well-known companies as General Electric.

WHY FRAUDS?

To understand the problem, we have to look at what fraud is and what it is not. Fraud is a type of non-violent crime for profit. This simple-minded definition seems hardly worth putting on paper, but if we examine exactly what it means, we'll get a better understanding of what we're fighting.

The basic motivation for fraud is to make money. There are all sorts of ways of earning money, just as there are all sorts of crimes. The two fit together quite well. However, in this country crimes of violence carry severe penalties, and only the lowest, least-educated classes of criminals commit them. It seems easy to rob a bank, but that carries with it a Federal rap, and the FBI inevitably comes into the case. There is also the risk of a murder, which despite the rarity of the death penalty, is still a very serious charge.

The fact is that crimes against property have lesser penalties than crimes against the person. We value human life highly, and crimes that injure people are, under our laws, the most serious, whether they are for profit or not. Some crimes against the person have great emotional charges, and we can expect a judge to "throw the book" at a child molester more than a bad-check artist.

Prisons are full of violent criminals. There are several reasons for this:

- Violent criminals tend to be stupid, and more easily caught.
- Violent crimes attract more attention, tend to be more sensational, and get higher priority from the police.
- Generally, there are longer prison terms for violent crimes, and those convicted spend more of their lives in prison.
- There is more sympathy for the victim of a violent crime, and judges tend to hand down stiffer sentences.
- With prison overcrowding, parole boards are often enacting early release programs for convicts. They tend to release those who in their view pose the least danger to society. Nonviolent criminals tend to get earlier paroles.
- Perhaps most importantly, many frauds are not even in

violation of an enforceable statute, which makes conviction much harder.

MYTHS ABOUT FRAUDS AND VICTIMS

There are several myths about frauds, and the characteristics of victims, which have been floating around for years. These myths came about from a superficial understanding of how fraud artists work, and from ignorance of the varied methods they use. Let's take these apart one by one:

You can't cheat an honest man. False. You can cheat an honest man, if your scam is properly targeted. This myth is based on the naive idea that the only people vulnerable to fraud are those who are greedy, and who expect to get something for nothing, laying themselves open to the false promises of the fraud artist.

In fact, even people with the highest morals and the most modest ambitions are open to fraud. A good example is the "bank examiner swindle,"¹ in which a person claiming to be a bank examiner asks the victim, who has an account at the bank, to withdraw a large sum of money to help the examiner check up on the honesty of a teller who is under suspicion. The victim does not expect personal gain, but is simply seeking to aid the examiner in enforcing the law.

Another scheme which involves victimization of people who are not seeking great riches is the "Social Security" or "Welfare" investigator scheme, in which a person claiming to be an investigator for one of these agencies arrives at the home of someone who is retired, or on welfare, presents phoney credentials, and claims to be collecting overpayments.² The "investigator" demands that the victim hand over to him or her the amount of the overpayment.

Frauds all involve get rich quick schemes. This is a corollary to the first myth, and it too, is false. While it is true that a person who shows raw, naked greed lays himself open to this sort of deception, there are also many victims defrauded because of need, not greed.

The fake employment-service swindle, in which a job seeker pays the fraud operator a fee to cover the cost of a "background investigation,"³ is a clear example of defrauding the needy. Another is the classic security-bond swindle, in which respondents

to an ad offering a cashier's or teller's job are asked to put up a large sum of money as a security bond because the purported position involves handling large sums of money and the "employer" wants tangible evidence of good faith.⁴

The victim of a fraud is somewhat stupid. Again, not necessarily. Our Twentieth-Century society is so complicated that it is literally impossible for any one person to be knowledgeable about everything he faces in daily life. Many successful operators exploit this, and offer products or services that pertain to the latest **developments in technology, or trendy fields.** In the early 1960's fast operators were selling nuclear bomb shelters. More recently there has been a rash of solar energy device sellers cashing in on one of the latest trends. "Survival" foods and supplies are another instance in which attaching a trendy label to ordinary merchandise enables an operator to hike the price to several times what other outlets charge for the same items.

From this we see that it is possible to defraud even knowledgeable and sophisticated people because there are inevitably some areas in which even the cleverest person lacks the technical knowledge to evaluate the worth of a product or service. Another point is that, in many fields such as the stock market, the rules are so complicated that only an expert can understand them and those outside the field are at the mercy of the specialists.

Frauds involve only shady, fly-by-night operators. It is not true that frauds are perpetrated only by sleazy types who have no fixed address or established reputation. A recurring theme in this study of fraud is that the fraud artists operate on the borderline of legitimate business, and that in many cases there are legitimate businesses that operate in a fraudulent manner. We shall see, in examining the medical profession, employment and literary agencies, and other established businesses, that they often engage in practices which are technically legal, but have a foundation of deception.

An equally important point is that fraud operators often assume the trappings of long-established and legitimate concerns. An operator will set up a front that uses a name very much like that of

a well-known company, and may even establish a well-appointed office which he claims is a branch of a real corporation.

NOTES

1. *Short Cons*, Scot Tinker, 1977, Eden Press, P.O. Box 8410, Fountain Valley, CA 92708, p. 7.
2. *Ibid.*, p. 8.
3. *Crooks, Con Men, and Cheats*, Eugene Villiod, 1980, Gambler's Book Club Press, Box 4115, Las Vegas, Nevada 89106, p. 57.
4. *Ibid.*, p. 58.

CRIME PAYS

This is an undisputed fact. Despite there being more people in prison today than ever before, crime still pays. However, we have to be careful to observe the limits, because not all crime pays. A jealous husband who murders his wife or lover is not doing it for profit, and gains only a temporary satisfaction, which he may later decide wasn't worth it.

To be precise, we should say that "crime for profit pays." Within this definition, there are all sorts of crimes for profit. Mugging and armed robbery are crimes for profit, but in relation to the risks of apprehension and the harsh penalties, they do not pay very well.

The gain from violent crimes is uncertain in most instances. "Great train robberies," in which the perpetrators get away with enough to retire for life, are very few. Mostly, violent crimes for profit are grubby gas station stickups in which the gain is a few hundred dollars at most, or muggings in which the gain may be only one or two dollars.

The risks are severe. An armed robber may be shot dead by the shopkeeper or by the police. Upon arrest, an armed robber is less likely to get bail than a non-violent criminal. Prosecution is easier, as there are few gray areas in violent crime. Sentences are longer. The prospect of parole or pardon is dimmer.

The smartest criminals are those who live by their wits. For them, crime really pays.¹ In many instances, the main reason is that many non-violent crimes are difficult to trace and prove. In fact, many are not even covered by the criminal code, but fall under the civil code.

A look at a few examples will illustrate the range of non-violent crimes and the difficulty of prosecution:

You are a storekeeper who accepts a bad check. The man who gave it to you had the required I.D., but it was false. You deal with many customers daily, and can give the police only an uncertain description, which makes the chances of his apprehension poor. Writing a bad check is a felony, but it is hard to enforce in practice.

You're shopping for a used car. The salesman tells you that the car you're scrutinizing is in good shape and well-maintained. It looks good to you, and is clean. You buy it, and find out later that it needs extensive repairs. The bill of sale states clearly that there is only a thirty-day warranty on the car, and the thirty days are up. You feel that the salesman misled you, and you're also kicking yourself for not having the car checked out by a mechanic before buying it. You have no recourse and have to eat your mistake.

You take out an insurance policy on your property. You suffer a loss and find that the insurance company will not pay you to replace it, although you insured it for your cost. The contract says, in the fine print, that the property is covered only for its depreciated value, while you have been paying premiums on its full value. The law stands on the insurance company's side, but you feel cheated because during the long discussion you had with the insurance salesman, he did not explain this to you.

You get an invitation to attend a showing of real estate tracts. The offer includes a dinner on the company, and you decide to attend, calculating that you'll at least get a free meal. You arrive at the office, and you and the other "guests" see a film depicting the property, which is several hundred miles from where you live and which you have never seen in real life. There are artist's renditions of a projected golf course, shopping center, and other improvements, and the salesman tells you that this property will be a good retirement site or investment for you. In front of you on the table is a pile of papers, which you start to read. The papers include sales brochures and a legal document. When you start to pick up the legal document, the salesman slams his hand down on it and continues to talk about the virtues of the property, making the offer seem so attractive that you sign a contract for it before you leave.

On your way out, you pick up the pile of papers. Upon reaching home, you look at the legal document, which is a statement by the state's real estate commission. This paper tells you that, regardless of anything the seller may have told you, you are purchasing the property at your own risk, and that there is no warranty that you are not purchasing a piece of swampland or a mountain peak, that

the property may or may not have utilities, and that you should physically inspect it before signing any contract. Slowly, you get the feeling that you've been had. You consult your lawyer, who tells you that you should not have signed anything before you knew exactly what you were buying. You're now committed to make the time payments.

A water-softener salesman comes to your door. He gives you a plastic bucket of "free samples" in return for your agreeing to listen to him for a half-hour. He shows you the effect of hard water on plumbing, etc., and convinces you that the unit he sells is the best on the market, saying that it has a lifetime warranty. You sign a purchase contract, and a few days later the unit arrives at your house, with a crew to install it. A month later, the unit breaks down. You find that to get it repaired, you have to dismantle it and ship it several hundred miles. There is no repair facility in town. Upon further checking, you find that a local outlet sells a similar unit for half the price, and that this company has its own service department, which makes house calls.

A salesman shows up at your door, claiming he is doing a market survey. He tells you he will give you a stack of records if you'll answer a few simple questions. You let him in, and he tells you that he is looking for new customers, and that if you give him the names and addresses of several of your friends, he'll give you a substantial discount on a stereo for yourself. You agree, and get out your checkbook. He brings in a stack of records and a stereo set in a cabinet. After he leaves, you look closely at the records and find they are "cheapies" by obscure artists, on unknown labels. Some days later, a friend who is familiar with sound systems tells you that the set you purchased is of inferior quality and that you overpaid for it. You never hear from the salesman again, although you find out a friend to whom you led him bought one of his sets. Some days later, your stereo fails. When you try to telephone the company whom the salesman represents, you find the number has been disconnected.

You answer an ad relating to an investment opportunity. A salesman calls on you, telling you that you have a chance to invest

in a company that will manufacture a new type of carburetor that doubles the gas mileage of any car. He shows you several brochures, and you think it is a good idea. You give him a check, he hands you a receipt, and you never hear from him again.

You answer an employment ad, feeling it is legitimate because the name of the company is familiar. When you arrive at the office, the “manager” tells you that you must invest some money to buy a stockpile of merchandise, and go on from there to build your own network of dealers. You sink a thousand dollars into this, and then find that persuading other people to buy the merchandise from you is far more difficult than you’d anticipated or been led to believe. Your lawyer tells you that you signed a contract that you would act as an independent dealer, that the parent company is not responsible for your success. You are left holding the bag.

Note that none of these schemes are ridiculous, something-for-nothing frauds. None of them involve anything outlandish, such as a machine for turning dirt into gold. None of them appear to involve any risk for the customer. None of them are even get-rich-quick schemes which promise huge profits instantly. They are all believable, which is why many people get taken in each year.

NOTES

1. *Crime Pays*, Thomas Plate, Simon and Schuster, New York, 1975.

WHY ARE WE VULNERABLE?

It seems shameful to admit we are vulnerable to fraud. It implies we are not very bright, that we can be outwitted. That is a degrading picture to paint of ourselves, yet to an extent, it is true.

It is a cliché that some of the sharpest minds in the country are working full-time to separate us from our money. Many of these people are not working at what most would call criminal pursuits. Those who work for advertising agencies, for example, are quite legally employed, even though their work is mainly devising new and more creative ways of telling lies.

Most of us have met people who seem to be natural-born schemers, whose minds are always working on ways to take advantage of someone else. Often, these people have very likable personalities, and inspire confidence, until we get to know them better. Most of us don't think along those lines, and thus are not prepared to resist a fraud.

Most of us do not seek to scheme, and do not even form the habit of thinking defensively. To most of us, transactions are straightforward affairs, in which we exchange a known quantity of money for a known product or service. Most of the time, we are not disappointed.

Another truism is that the world is a complex place, and life is getting more complicated every day. In daily life, we have to depend a lot on faith and trust. We assume without checking thoroughly that something we buy will be what we want. In buying a car, for example, we trust that it will get us from one place to another without breaking down, even though most of us are neither automotive engineers nor mechanics.

This is true of almost anything we buy. We cannot be specialists in everything, and cannot evaluate the quality of the many manufactured products we use each day. When we buy services, we are on even more slippery ground, as often we cannot evaluate whether or not we got our money's worth until after it is all over, and the best guide we have is experience with a certain provider.

Automobile mechanics are very variable in quality, and good advice is to stick with a mechanic we've found to be competent.

Medical care is another, and much more serious, problem. Finding a good doctor can be very difficult, and since medical care is such a complicated subject, it is hard for a layman to discern whether or not a treatment or drug a doctor advises is either necessary or effective.

This brief review of the problems we face in normal transactions provides a good background to the difficulties in preventing our falling victim to fraud. In our complex Twentieth-Century industrialized society, we are accustomed to accepting products and services from people we hardly know, or don't know at all. In some cases, we buy sight unseen, as from mail-order catalogs, secure in the knowledge that **most mail-order operators** are honest. In other cases, we buy intangibles, such as insurance, and we depend on the reputation of the insurance company.

Most transactions are not as straightforward as we'd like them to be, but we can't help that. It is easy to detect, in a supermarket, whether a container of milk is sour or if fruit is spoiled. It is much harder to decide if a manufactured product will give us good service. That is why we tend to rely on third parties, such as the publications of various consumer groups and the standards set by the government or industry associations.

The pace of life is faster. We are being constantly pressured to make snap decisions in our buying. Merchandisers often do not allow us the time to make a deliberate judgement, as they present "limited offers" and "one-day sales." We have become accustomed to deciding on the spot.

Most of us have the sense to know that a big purchase requires more thought than a small one, that buying a car is a greater commitment than buying a pocket radio, because we have much more to lose if we make a bad decision, but even in this we often find almost irresistible pressure to *buy now!* Car salesmen, whether working for new car dealers or used-car lots, have well-developed sales skills and high-pressure tactics to push us into signing immediately, even when they are selling a perfectly legitimate car in good condition.

As previously mentioned, the dividing line between legitimate business and fraud is so thin as to be invisible. The similarity in tactics between fraud artists and legitimate businessmen blurs the distinction further.

Now that we've surveyed the social factors that make us vulnerable to fraud, let's tackle the hard part, our personal traits. A former manager for the Fuller Brush Company said that "Door-to-door selling is the post-graduate course in practical psychology."¹ This is true of both the legitimate salesman and the fraud artist. The fraud specialist is expert at taking advantage of our weaknesses. He knows how to "read" a person and assess vulnerabilities. This is not a magical skill and is not perfect. One of the best-kept secrets of salesmen is how often they fail to make a sale. This is also true of con men. Most of us will resist a con game most of the time. The basic principle of strategy, both in selling and in fraud, is not to waste time on those who are unlikely to buy, and move on quickly to someone who is more vulnerable.

Both salesmen and con men know that all of us have certain characteristics which may make us vulnerable. This is what they look for, and what they exploit:

Mind-set. This is a preconceived attitude that sometimes leads us to false conclusions. Right now, with the controversy over energy sources, many people have a mind-set that solar energy is safe, non-polluting, and economical. This opens the door to many fly-by-night types who sell cheap and ineffective solar energy devices. Many people are also prepared to accept various types of energy-saving devices uncritically, enabling salesmen and con men to sell them cheap timers at high prices in the belief they will save on fuel bills.

Stereotyping. This is a combination of social and personal attitudes that makes us more ready to accept certain types of people and presentations. We see certain people as "respectable" and others as disreputable. We tend to have more confidence in a person who is neat and dresses well, drives an expensive car and has a well-furnished office than we do someone who appears "hungry." We also tend to listen with more respect to someone

who is articulate and well-spoken than to someone who has a poor vocabulary and uses bad grammar.

Allied with this are ethnic stereotypes. We are more likely to react positively to a person who is Caucasian, has an "American" sounding name, and speaks without an accent. This is changing, however, as each new generation grows up bringing with it new values.

Bargain-hunting. While most of us are sophisticated enough to know that we rarely, if ever, get something for nothing in the real world, and people do not give fortunes away, we still seek good deals. We know, for example, that it is possible for someone to buy stock in a company when the price is low and to make a profit by selling when the price goes up. We also know that prices in our "free-market" society are volatile and it is possible to get good deals by buying in the right place and the right time. Con men offer us spurious "good deals."

Suggestibility. Some people are prone to believe almost anything anyone tells them. Both salesmen and con men try to enhance suggestibility by appearing "respectable." Suggestibility warps judgement, and those who are very suggestible will often accept on "say-so" what the rest of us would not without further proof. A salesman or con man can tell a suggestible person by some physical signs. For example, someone who constantly nods "yes" while the pitchman is talking is showing suggestibility. Salesmen and con men also look for a gleam in the eye, a brightening of the expression, upon hearing of the "good deal."

Suggestibility can also be gauged by the person's willingness to accept the approach. Salesmen and con men never ring a doorbell and say they're there to sell a vacuum cleaner or uranium stocks. Instead, they tell a lie, claiming that they are conducting a survey, doing market research, or giving out gifts. Most of us know that when a stranger phones or rings the doorbell, he's not there to do us favors, but some accept this spurious explanation at face value. This gives the experienced salesman or con man an important indicator of his victim's suggestibility.

Laziness. Some of us are not especially suggestible, but are mentally lazy, and unwilling to do our homework in checking out

claims. We do not bother to ask the right questions when we're confronted by a "deal," and do not bother to investigate further than reading the sales brochure. Although it is usually possible to check with the Better Business Bureau, references, or the police, victims of frauds don't do this.

Possibly the most important reason we're vulnerable is that *fraud artists are pros and we're not*. An amateur is at a distinct disadvantage when up against a pro. We can't hope to prevail against a professional boxer, despite some experience while in school. Although most of us have driver's licenses, we cannot hope to match the skill of a professional race driver. In the same way, we can expect to fail when up against a professional con man, unless we have ways of compensating for our deficiencies.

NOTES

1. Personal statement to the author.

PORTRAIT OF THE FRAUD ARTIST

The stereotypical image of the criminal is a dull, brutish lout more at home with a gun or blackjack than with a good book. This is utterly untrue of fraud artists. Let's look at the real fraud artists and see why they are so successful.

The term "con man" is accurate. Fraud artists are skilled at building confidence in the victim. "Con man" is inaccurate in one respect. The fraud artist may be either male or female. It's a mistake to think that fraud artists are all fast-talking, shifty-eyed sleazebags -- on the contrary, they work very hard at looking respectable.

They tend to be very intelligent people. A common misconception, reinforced by those who preach that "crime does not pay," is that criminals are stupid, that they are low-life misfits who, if they had normal intelligence, would earn their livings honestly. In fact, fraud artists are among the elite of crime. It is mainly the stupid and untalented criminals who get caught and prosecuted successfully. The prisons are filled with failures in this field.

While it's true that street criminals tend to be young men who often straighten out after they mature completely, the picture is quite different in the realm of fraud. Fraud artists tend to be dedicated professionals, true career criminals who, if they are imprisoned, return to their preferred method of livelihood.¹ Fraud artists tend to be winsome, attractive people. They certainly are "street-wise," a skill which is of utmost value in conning the victim as well as conning the parole board in the unlikely eventuality of conviction and imprisonment.

They are good actors. Although probably unable to play serious roles upon the stage, their performances are tailored to the roles which they play in real life. This puts the victim at a disadvantage, as he is up against a "pro."

Perhaps most importantly, their performances and tactics are well-rehearsed. They work hard at perfecting their skills. They can

put across a complicated deception without the guilt and unease the rest of us feel when telling lies.

NOTES

1. *Fraud Investigation*, Glick and Newsome, Charles C. Thomas, 1974, 2600 S. First St., Springfield, Illinois 62704. p. 8.

ANATOMY OF A FRAUD

We can dissect the operations of a fraud artist into component parts, in order to understand not only the basic deception but the dynamics of the process. Fraud is a transaction, an interaction, between two parties, and its success depends on some subtle and often intangible factors.

INCENTIVE

This is the first component. The victim must have an incentive to place himself in the hands of a fraud artist. In the classic swindles, the con man makes the initial approach, offering his get-rich-quick scheme. This is not always so, however. Some victims are lured by impersonal approaches, such as advertisements and word-of-mouth. It might seem strange that one fraud victim might give a recommendation to the fraud artist, but some fraud schemes are partly based on this, as we shall see. In other instances, a fortune-teller or faith healer may give the victim great satisfaction, and win a convert.

The incentive is usually some sort of benefit for the victim. It's a mistake to think this is always a tangible profit. Sometimes the motive is health and well-being, sometimes the good feeling that comes from helping others, as when making a gift to charity.

THE COME-ON

This is reinforcing the incentive. The con man establishes confidence in the victim, sometimes by presenting credentials, in other instances by sheer force of personality and salesmanship. The skills involved are exactly the same that salesmen and other more or less legitimate people develop.

THE SHILL

This is a third person, sometimes unwitting, but more often part of the scheme. A shill acts as a disinterested party, reinforcing the victim's participation. He can be a fake buyer at an auction, serving to bid up prices. He can be a supposedly unrelated third party in a pigeon drop. He can be a contributor in a "flop" scheme, etc., as we shall see.

THE SWITCH

This is the substitution of a fake for the article of value, which forms a part of many schemes. Sometimes the switch is as crude as substituting a lead brick for a gold brick. In other cases, there is no physical switch involved, but an intangible one, as in bait-and-switch advertisements.

PRESSURE

The con man often uses some form of pressure, to hurry the victim along and impede him from carefully considering the transaction. He often imposes a time limit, either by stating that the deal is a now-or-never offer, or by claiming that there is another buyer waiting, possibly with a better offer. This is why those who engage in con games are sometimes known as "hustlers."

THE BLOCK

This tactic is aimed at stopping the victim from reporting the incident to the police, and is often a carefully-planned part of the scheme. The victim might buy an item which he thinks has been smuggled, for example, in which case reporting to the police would involve a confession of wrong-doing. In other instances, the activity, while perhaps not outrightly illegal, is shameful. Schemes involving sex play upon this.

In yet other instances, the victim supplies his own block. Many instances of fraud go unreported because the victims are ashamed to confess that they have been outwitted. If the sum involved is small, the victim may decide he'll just write it off to experience.

Some schemes use anticipation of further reward as a block. In referral and commission schemes, the con man, by promising, and sometimes paying, commissions for prospects referred by the victim, turns him into an unwitting *steerer*, or *shill*.

Some victims never complain because they never realize they've been defrauded. A victim who buys a fake diamond, for example, may never have it appraised, and never find out it is bogus.

The block need not be permanent for it to succeed. For the con man's purpose, it need only keep the victim quiet for a limited time, enough for the con man to get out of town or to work his scheme on other victims.

Con games, although they vary greatly in style and substance, are all simply permutations of these basic elements. Con men are constantly thinking up new games, or new variants of the old ones.

ONE STEP AHEAD OF THE LAW

It's a fact that non-violent crime is more profitable than violent crime. It's also a fact that it is harder for the criminal justice system to cope with non-violent crime, and there are both fewer convictions and lighter penalties. In the case of fraud, judges and juries have a prejudice against the victim, seeing him or her as a victim of their own stupidity as well as of the criminal's scheme.

Fraud is an intellectual crime, not a physical one. It takes more brains to plan and carry out a fraud scheme than it does to execute a mugging. Except for the higher level of intelligence required, the mentality of the criminal is the same. He or she sees other people as prey, to be harvested for profit.

One important part of the problem is that the law often seems to be a step behind in coping with frauds. Violent crime is clear-cut and easily identifiable. Fraud often is not. This is the crucial point which makes apprehension and prosecution more difficult.

The criminal justice system is reactive. There must first be a crime; only then can the system act. Thinking about committing a crime is not an indictable offense. Planning is, but proving conspiracy is very, very difficult.

A major component of the fraud artist's planning is in thinking up a scheme that will be difficult or impossible to prosecute. While there are laws on the books regarding fraud, the schemers are constantly thinking up new plans, and given the slow pace of the law enforcement authorities and the legislators, the laws covering frauds are usually one or more steps behind the acts.

Computer crime is an excellent example. There have been many, some of which remain undetected. There are few laws on the books covering computer crime, despite the warnings given by computer security experts. There is the typical lag between the discovery of a new type of crime and the implementation of a law to cover it.

The key to fraud is there is a willing victim. There is no coercion involved. For a criminal prosecution, it is necessary to prove intent to defraud, and sometimes the fraud operator can claim that the

affair is simply a disagreement over the terms of a contract, which makes it a civil, rather than a criminal matter.

Just as the dividing line between legitimate business and fraud is very thin, the line between fraud and deception is also almost invisible. A fraud artist who tries to peddle a machine that changes one-dollar bills into twenties can definitely be indicted for fraud, but a company whose advertisements promise us that if we buy its product we will be happy cannot. Yet, there is deception in each instance.

One major reason for the slowness of the criminal justice system in responding to fraud is that in this country, the legislators are business-oriented. They are very reluctant to pass any law that may affect legitimate business, and only the most flagrant abuses will move them to act.

One example is the "Truth In Advertising Act." The shades of deception, and outright lies, promoted by advertisers finally became so notable that the United States Congress, after decades of neglect, passed a law.

Another example is the "Truth In Lending Law." Banks and finance companies had for generations concealed the true rates of interest from their customers until it finally became necessary to make it mandatory to disclose what the consumer would actually pay for the credit.

Only recently have there been laws that spell out precisely that certain previously common practices, such as turning back the odometer of a used car, are fraudulent and illegal. The reluctance and slowness of the government in reacting to fraud is one of the things which open the door to the creative fraud artist.

This background shows us the task of the fraud operator who succeeds: He finds a scheme that will earn him money, but which is not easily indictable because there is no law spelling out that what he's doing is illegal, although his intent is to deceive. The fraud operator who gets rich and stays out of prison is truly one step ahead of the law.

CLASSIC SWINDLES

Let's start our study of frauds by examining the classic swindles, the "oldies but goodies." These scams are very old, yet we find them still in use today, sometimes in their original versions, and sometimes with modification to bring them up to date.

Inevitably, the question comes up: "Why do these old scams still work?" The schemes are old, but the operators use them on new people, as each generation has to learn for itself the problems and mistakes that plagued its ancestors. P.T. Barnum allegedly said of suckers: "There's one born every minute," and he was right.

THE SPANISH PRISONER

This is the oldest known swindle, allegedly dating from 1588. The swindler approaches his mark with a letter, supposedly written by a person unjustly imprisoned in a Spanish castle. The letter states that a certain amount of money, which will serve to bribe his jailers, will secure his release. The letter also alleges that the prisoner has a treasure chest full of valuables, which he will share with the person who puts up the money for his freedom. The victim hands over the money to the swindler, who disappears.

It might seem incredible that anyone would fall for this today, but there are modern versions, as swindlers keep up with the times.¹ One is that the prisoner is incarcerated behind the Iron Curtain, or in a "Third World" country. The money requested may be for bribes, or to hire a force of mercenaries to mount a commando-style raid to rescue the prisoner. The treasure chest story is old, and the modern version is that the prisoner has a cache of bearer bonds, or a numbered account in a Swiss bank. The swindler tailors his story to the needs and fashions of the moment, which enables him to get more mileage out of an old con game.

THE PIGEON DROP

This one is only perhaps 200 years old, according to one source.² The victim “accidentally” runs into the con artist on the street and they strike up a conversation. They soon find, as they are walking along, a wallet or pocketbook, or even a paper bag with a large sum of money inside. There is no identification in the wallet, and it seems they can keep the money with clear consciences. The con artist suggests that, to be on safe ground, he consult his lawyer to find out exactly how the law regards found money.

The con artist returns from the lawyer’s office, saying the lawyer informed him or her the two finders are legally entitled to the money if nobody claims it, but that each must put up a “good faith” bond to establish their honest intentions and prove that they can return the money if it is claimed by the person who lost it. The victim withdraws a certain sum of money from the bank, hands it to the con artist, who claims that he’ll deliver it to the lawyer to be put into an escrow account, and the victim never sees the con artist or the money again.

There are many variations possible in this swindle. The con artist may ask the victim to accompany him to the lawyer’s office so they may both hear what the lawyer has to say. The lawyer takes charge of the money, and the victim returns with the “good faith” bond and places it in the lawyer’s hands. The lawyer says if the money is unclaimed after six months, the finders can split it. This tactic enables the con artist and the “lawyer,” who is his confederate and not really a lawyer, to work the scheme many times from the same rented office while their first victims are waiting out the six months. When the first victim returns to the “lawyer’s” office, he or she finds the occupant has moved and left no forwarding address.

Another variant is the con artist asks for a bond from the victim, meanwhile giving the victim the package of money to keep in his safe deposit box. This deception involves the use of a “Michigan roll” or “gambler’s roll,” which is a roll of paper cut to the proper size with a few genuine bills on the outside. The original “find” may be real money, and in fact has to be if the swindler switches

wallets, or packages, leaving the victim with the fake roll. They both go to the victim's bank, and the victim puts the fake package in his safe deposit box. He then withdraws the amount for the "bond" from his account, feeling safe because the amount of the "bond" is less than the amount supposedly in the package. The swindler then disappears.

THE ENVELOPE SWITCH

This old game usually requires a con artist and a confederate. A likely spot for the initial meeting is a bar, in which the artist strikes up a conversation with the mark. The con man claims to be a seaman, traveling salesman, or otherwise a stranger in town. He mentions that he wants to have a good time on his first night in town, and says he intends to go to a certain locale or to a house of prostitution. At this critical juncture, the confederate, who has been sitting nearby, comes into the conversation and tells the con man that he runs the risk of being robbed or "rolled" if he ventures into that part of town.³ He suggests he leave the bulk of his money with the mark for safekeeping. The con man agrees, but suggests that the mark take the money and place it in an envelope, adding a matching amount from his own funds to ensure that he will be careful not to lose the envelope. If the mark agrees, the shill produces an envelope, into which he places the money in front of both the victim and the con man. The mark may not have enough money, in which case he may make a trip to the bank to make a withdrawal. This game, in earlier years, had to be worked only during banking hours, but today, with the common use of electronic teller machines, is possible at all hours of the day or night.

Both the con man and his shill watch the victim start to place the envelope in his pocket. The con man snatches the envelope back from the mark, telling him that the safest place to keep it is inside his shirt, and in the process opens his shirt and puts the envelope inside, as if to demonstrate the proper carry. This is where he makes the switch. Inside his shirt is another envelope, filled only

with paper cut to size. He hands this envelope to the victim, who then places it inside his own shirt. The con man asks the victim for his address, so that he may recover his money later, thanks the victim for his help, and leaves to have his night on the town. The confederate says his farewell and leaves shortly thereafter. Sooner or later, when the con man does not show up, the victim opens the envelope to find he has been taken.

THE MURPHY MAN

In this swindle, which is most suitable for use in a large city with many out-of-town visitors, the "Murphy" man approaches a visitor and suggests that he can get him a woman for the night. Posing as a pimp, he quotes a price to the victim, and asks for the money in advance. The victim pays him, and the con man leads his mark to a hotel. Asking his victim to wait for him outside, or in the lobby, the Murphy man says that he will go upstairs to conclude the deal with the woman and to assure that she is free for the night. He then leaves by another exit. To reassure the victim, he may even tell him the room number, and instruct him to come up after ten minutes.

THE GOPHER SWINDLE

This requires a con man and an assistant. The con man, well-dressed, appears at a hotel, restaurant, or gas station, and asks where the men's room is. He returns a few minutes later, telling the clerk he has lost a very valuable piece of jewelry, and asking his assistance in searching for it. The clerk accompanies the con man, and together they search the premises to try to find the lost jewelry.⁴ They fail, and the con man tells the clerk the jewelry is very valuable and he'll pay a substantial reward for its return. Pleading urgent business, he leaves, but gives his business card to the clerk.

Sometime later, the accomplice comes up to the clerk, shows him a piece of jewelry which matches the description of the missing

item, and claims he found it on the floor. The clerk tells him it was lost, and that he knows the owner. The finder refuses to give up the jewelry, claiming "finders keepers." At this point, in the belief that he'll still earn a good amount of money from the transaction, he offers the finder a price, the finder accepts, and hands over the item. Anticipating a large profit, the clerk telephones the number on the business card, to find it is a fake.

THE FLOP GAME

In this old con, a shabbily dressed person collapses on the street during rush hour. A well-dressed man, claiming to be a doctor, approaches and examines the person, around whom a crowd has gathered.⁵ The victim starts to speak, claiming to be out of a job, not eaten for three days, and having small children at home to whom he or she has given the last of the food. The doctor announces to the crowd that it is a disgrace that, in the richest country in the world, anyone should starve. He takes off his hat, drops a large bill into it, and passes it around for contributions from the onlookers. After the bystanders have made their contributions, the "doctor" thanks them, helps the victim up and says he will help him or her get home.

THE CARD GAME SWINDLE

There are several variants on this old and successful swindle.⁶ The con men rent a room at a hotel that is hosting a convention, start a card game, and invite some of the conventioners to join. The con men explain that, because of local ordinances against gambling, money cannot appear on the table, and the players must buy chips from one of them. They have a cash box, from which they take chips and into which they deposit the money.

In one variant, one of the con men pretends to become violently ill, and the other con men offer to take him back to his room, telling the marks to watch the cash box carefully. They do not

return, having at some point during the session emptied the money or switched cash boxes.

In another version, the game is interrupted by the entry of "detectives," who claim to be from the bunco squad and who inform the marks that they are about to be taken by professional gamblers running a crooked game. They handcuff the con men, pick up the cash box, and leave, explaining to the marks the cash box is evidence but as they are innocent parties, they can claim their money at the police station the next day. The fake policemen leave with their prisoners and the victims have lost their money.

THE GOLD BRICK

This one is "old enough to have whiskers" but presumably it or a variation on the theme is still in use. The con man offers to sell the sucker a gold brick. To allay suspicion, the con man advises the sucker to have the ingot assayed, and in doing so the sucker finds out the metal is genuine. He pays the con man for it, and at some point during the proceedings the con man or an accomplice make the switch, substituting an ingot of base metal for the gold one.⁷ Sometimes, the con man switches the bricks before consummating the deal, and in other instances when the mark is staying at a hotel, he lets himself into the victim's room with a passkey and makes the switch then.

THE SECURITY SWINDLE

This is a game the con man can play with many different pieces of merchandise. In one case, the item is a violin.⁸ The swindler comes into a store, gas station, or other business, and buys a small item. He repeats this a few times, to become known to the proprietor. He then tells the businessman that he is broke, and asks if he can leave his watch, his violin, or other valuables as security for another small purchase. If the proprietor agrees, the con man leaves the piece. For this to succeed, the item left for

security must be left out in plain sight by the proprietor, perhaps hanging on the wall or in a display case.

Some days later, the con man's helper, dressed very well, comes into the place of business. He sees the item, and asks how much the proprietor wants for it. The sucker explains that it is not his to sell, as it was left for security by a customer. The accomplice tells the mark this is a very valuable item, and that he'll offer a large sum of money for it if the person who left it abandons the item. He leaves a business card, and departs. Later, the con man returns with his tale of woe. He lost his job, or cannot find a job, and is desperate. He asks the patsy if he would be willing to buy the item from him, as he cannot redeem it. He asks what seems a low price for it, but actually is much more than it is worth. The businessman, calculating that he'll make a handsome profit, accepts the deal and pays what the con man asks. When he tries to get in touch with the well-dressed potential buyer, he finds that he cannot, because the card is a fake.

PANHANDLING

Panhandlers have been around for centuries, sometimes known by other names such as beggars, bums, and tramps. Many of them are simply down-and-outers, who beg for coins to buy a meal, and usually spend it on cheap wine. There are some who earn very good incomes, however, because they have systematized their panhandling so that it is almost a science. One very successful panhandler allegedly had a home in a wealthy suburb of New York, and a wife and children who believed that he was a well-to-do-stockbroker. Each day, he would drive into Manhattan in his Cadillac and park it in a midtown garage, where he would remove his business suit and put on shabby clothes that he kept in the trunk of his car. He then would go out on the streets, having learned from experience which were the best locations. He had his approach well worked out, and from long practice, could intuitively select subjects who would be susceptible to his begging. He would collect a coin or two from each one. None of the people he approached would give him a significant amount of money, but

the key to his technique was that he made many “scores” each hour. During an eight-hour day, he would collect as much as if he had actually been working as a stockbroker. At the end of each day, he would return to the garage where he had parked his car, change into his suit, and drive home to his family in Westchester.⁹

There are many variations on the panhandling theme. Another type is the well dressed man who approaches his victim in an embarrassed manner and claims to be a businessman from out of town who has overspent and is now out of money, or who has been robbed.¹⁰ He has no cash or credit cards, and no money to wire or phone his company or relatives for help. If the sucker bites, he’ll lend the con man a substantial sum of money.

Another variant is for the well-dressed “businessman” to make the rounds in an office building, explaining that he is in town on a business trip and admitting that he had too much to drink the night before, and was robbed while intoxicated. This sympathy story will get him many “loans” from credulous victims.

THE INTENTIONAL VICTIM

This theme covers a lot of ground, the object of the fraud being to set someone else up for a lawsuit. One type, well-known to insurance companies, is the “leg-breaker,” the person who is “accidentally” hit by a car, or who breaks a leg “accidentally” in a building. Working in collaboration with a lawyer, who is usually part of the swindle, the “victim” becomes the plaintiff in a lawsuit. The physical injury is, in the view of the swindler, a cheap price to pay for the large settlement that usually results.

One reason for the proliferation of “whiplash” claims in recent years is this sort of injury is very hard to disprove, and so there is no need for a fraud artist to sustain a severe physical injury or secure the cooperation of an unethical doctor.

Insurance companies are very much aware of this type of swindle, and employ staffs of investigators to verify the claims against them. One of their most valuable tools is a file of the names of people who have brought suit before, which cues them to those

who make a career of injury claims. While it is true that a “flop artist” can assume a new identity for the next “job,” an investigation can often reveal whether or not the claimant’s identity is genuine.

Another variant on the lawsuit theme is to set up a businessman for a lawsuit for false arrest. In its simplest form, the con artist enters a store which he knows employs private detectives to counter shoplifters. He behaves furtively, and pretends to slip merchandise into his pockets. When he’s sure that he has attracted the attention of one of the staff, he heads for an exit. An accomplice remains nearby, to serve as a “witness.” When the detective arrests him, the con man protests his innocence, and makes a scene, being careful to keep his protest verbal and non-violent. He refuses to submit to a search, and the store detective sends for the police to lodge a formal complaint. When the police arrive, and place the “shoplifter” under arrest and search him, they find no evidence on him. With his case fortified by his “witness,” the con man can either sue or accept a settlement out of court.

As with personal injury cases, insurance companies keep detailed files of the plaintiffs, and freely exchange information for mutual protection. This is one reason a person who applies for a policy, or makes a claim against an insurance company, will have his name in the files of many, or in a central bureau. This practice has led to apprehension about “Big Brotherism” and the files kept on honest citizens. The reason for the extensive record keeping is innocuous, merely a self-protection measure by the insurance companies.

Yet another method of setting up a merchant for a false arrest suit is for the con man to buy a valuable piece of merchandise, for example a watch, and pay for it by check. He then goes into the shop next door and tries to sell it, usually for far less than he paid for it. He suggests the proprietor check on the value of the watch with the jeweler next door. The jeweler becomes suspicious, and confronts his client, demanding to know why he is trying to sell a watch he has just bought, thinking the client bought the watch with a bad check and is now trying to get rid of it. The “client” feeds his suspicion, saying that he changed his mind about needing

a watch. The jeweler asks for the watch back, and the con man refuses, further inflaming the jeweler's suspicion. At this point, the jeweler sends for the police, and an arrest ensues. The police investigation discloses that the check the con man gave the jeweler was valid, and that sets the scene for a false arrest suit.¹¹

THE RICH LADY SWINDLE

An elegant and well-dressed lady buys a lot of merchandise at a store which carries only top-line items. When it is time to pay she tells the clerk or proprietor she has forgotten her wallet and checkbook, and cannot pay. She suggests that the sucker accompany her home, where she will settle the bill. She says her limousine is outside, and she'll have her chauffeur return the mark to the store, to help make up for the inconvenience. They load the merchandise into the car, and drive to a wealthy neighborhood, where they start to get out of the car. The lady hands some of the merchandise to the merchant, filling his arms, and tells him to ring the bell so the maid and butler can help get the rest of the packages inside. As he reaches the doorstep, the merchant hears the car drive off, and he loses the merchandise still in the car.¹²

A SIMPLE MAIL FRAUD

An advertisement appears, offering a coat hanger and a cigarette lighter for a price. The victim mails the money to the address listed, and a few days later receives an envelope containing a match and a nail.¹³

THE FAKE COLLECTION AGENCY

A businessman with long overdue bills answers an advertisement for a collection agency. When he arrives at their office, the "manager" tells him they do not collect their fee until they recover the debt, and their fee is a modest 15%. The businessman agrees, and hands over his delinquent invoices. The

manager hands him some legal papers to sign, telling him that they are powers-of-attorney and authorization forms. When the businessman has signed them, the manager tells him he will have the papers notarized and filed with the authorities the same day, and asks the businessman for the required fees, which are modest. Upon receiving the fees, the manager sends one of his subordinates out to have the papers processed.

As the weeks go by, the businessman, if he inquires, will hear from the manager that the agency is still working on the debts, and that they expect results soon. One day, he finds that the phone is disconnected, and a visit to the "office" tells him that the occupants have moved, leaving no forwarding address.

The confidence ring has been systematically collecting "filing fees" from all who sought its services, and the large number of clients paid sums that added up to a substantial amount.¹⁴

THE INVESTMENT FRAUD (PONZI SCHEME)

The swindler advertises that he can offer very substantial returns to very modest investors. An investment of five hundred dollars, for example, will yield the investor dividends of one hundred dollars a month. The sucker who answers the ad may think this is too good to be true, but the next month he gets a check in the mail for one hundred dollars. The following month he finds another hundred dollar check in his mailbox. The next month he finds that indeed it was too good to be true, as no check arrives and when he goes to the office of the investment company he finds it empty, with no trace of the occupants.¹⁵

There are two variants on this swindle:

One is to pay back part of the money invested, still making a profit on the transaction, three hundred dollars in this example.

The other is to make payments to keep the sucker satisfied, not only to allow time to get out of town, but to encourage him to send the con man new clients, offering a bird-dog fee of one hundred dollars for each one. This pyramids the sales, and the con man uses

the new investments to pay off the old clients in installments, until he feels he has exhausted the local market.

THE FORTUNE-TELLING SCAM

While many people believe in psychics, fortune tellers, and other “readers” and pay modest sums to get advice and predictions of the future, some are victimized on a large scale by outright con artists. The method is as follows:

The victim visits the gypsy lady, who tells her the root of her misery is money, and she can cleanse herself of her hard luck by destroying some of it in a special ceremony. She instructs the mark to bring a large sum of money on her next visit. When the victim shows up with the money, the gypsy places it in an envelope and chants prayers over it. At some point during the ceremony, she switches the envelope for one containing only pieces of paper cut to the size of the bills. Then she places the envelope in the fire, and says more prayers. At the end of the session, she tells the victim that the evil spirits have been cleansed and her life will be better from now on.

Sometimes the deception involves the victim’s jewelry, if the victim is affluent enough to have valuable pieces. The gypsy tells the mark to bring them with her, and she’ll keep them for several days and return them cleansed of evil spirits. After several days go by, without the return of the jewels, the victim finds the gypsy has folded her tent and moved on.¹⁶

SNAKE OIL

Patent medicines have a bad name for some very good reasons. They have been sold at carnivals, by door-to-door salesmen, and in local stores. They are usually useless concoctions, but there is no difficulty in finding people who swear that a certain medicine worked for them, because the human body heals itself in most illnesses, with or without the remedy.

Patent medicines are only one manifestation of the charlatanism that has been a part of health care since prehistoric times, and although government regulations have driven out some of the more blatant snake oil salesmen, who used to award themselves medical degrees to lend authority to their sales pitches, the recent problems with the “starch blockers” shows us the field is not yet closed. We will examine these problems more closely in the chapter on health care.

TOUTS

The tout is a tipster, who passes betting tips to his victims, extracting the promise that they’ll split the take with him if it pays off. Touts work at race tracks, betting halls, and even stockbroker’s offices, among the clients watching the big board. The tout approaches his victim, starts up a conversation, and soon claims that he is very experienced in the field, or has inside information, and offers to pass on tips to the victim, in return for a promise to split the winnings.

The tout does not have to know very much, as his scam does not depend on any ability to predict winners. He works by making different predictions to different people, knowing that just by the laws of chance, some of his tips will be valid. When one of his winners comes in, he seeks out the person whom he tipped off and collects. Meanwhile, he avoids the losers.

Touts make the round of tracks, betting offices, and financial centers around the country. They can’t work a particular locale for long, because of the prospect of an unpleasant confrontation with a victim, or even arrest and prosecution.

THE OLD SCAMS LIVE ON

With this quick survey of classic frauds, we’ve seen how old ideas linger in the minds of confidence artists, cropping up again and again as each new generation of potential victims arrives. Some of the classics need cosmetic work, to keep up with changing times, but the basics remain the same. Technological innovations

dictate some changes, and help bring about new con games and swindles, but the fundamental principles of deception, of preying on the weaknesses of human nature, never change.

NOTES

1. *Short Cons*, Scot Tinker, Eden Press, 1977.
2. *Ibid.* p. 5.
3. *Ibid.* p. 6.
4. *Ibid.* p. 26.
5. *Ibid.* p. 27.
6. *Ibid.* p. 34.
7. *The Bunco Book*, Walter B. Gibson, 1976, p. 4.
8. *Ibid.* p. 5.
9. Related to author by a professional panhandler.
10. *Bunco Book*, p. 10.
11. *Ibid.* p. 22.
12. *Ibid.* p. 25.
13. Related to author in elementary school by a teacher who was near retirement age. This one is old!
14. *Bunco Book*, p. 68.
15. *Ibid.* p. 70.
16. *Ibid.* p. 72.

ADVERTISING FRAUDS

Most of us are familiar with the petty deceptions and outright lies that many advertisers use routinely. We've been exposed to the many commercials on television that promise us we will be sexier or happier if we use a certain cosmetic, drink a certain brand of beer, or buy some other product. This constant exposure desensitizes us to exaggerated claims somewhat, and we often simply don't respond to the claims. In fact, many advertisers are distressed that TV watchers use commercial breaks to go the bathroom or kitchen.

There are some flagrant frauds on TV, most of which operate only for short times, until the slow-moving mechanism of law enforcement catches up to them. Most of us have seen commercials for overpriced items available by calling an 800 number displayed on the screen, and realize we can buy the same or better quality products for less at local stores.

A recent variant is diet pills, supposedly with newly discovered ingredients, which are guaranteed to work. The wording of the guarantee is the interesting part, and the crux of the scheme. The viewer can, by calling an 800 number, obtain a supply of the diet pills for twenty dollars. If he is not satisfied with the results, the vendor will give him another supply of pills, at no cost, providing he pays the handling and shipping, which comes to about three dollars. The pills are the same that sell for about three dollars in drugstores and supermarkets. The initial purchase earns the advertiser a huge profit, and subsequent sales give him the normal profit enjoyed by retail outlets.

We learn from experience that most advertising claims are lies of one sort or another, sometimes outright criminal frauds and other times based on unproven assumptions regarding certain trendy products or substances.

About twenty five years ago, a small company in New York added shoe polishing cloths containing "silicon" to its line of notions. The claim was that the "silicon" contained in the cloth would help obtain a higher shine. In fact, the cloth strips were

simply trimmings from the material used for ironing board covers, which would have gone out with the trash otherwise. This material has a hard, silver finish on one side, and a soft backing on the other. The soft backing did indeed work well in shining shoes.¹

Buying goods sight unseen is a risky practice. It's not necessary to go into great detail and enumerate the instances in which shoddy merchandise sells through TV or other advertisements which do not allow the buyer to inspect the goods in person. While there are honest mail-order houses which have established reputations for fair dealing over a long time, there are also fly-by-night operators with compelling offers that seem too good to miss. These are the ones which offer the greatest risk.

NOTES

1. Personal knowledge of the author, who in his youth worked at this company for three months. The vice president, an affable man, admitted to the author that the claim of "silicon" was a "gimmick."

BUSINESS FRAUDS

While all frauds involve some sort of business, some are especially aimed at companies, where they take advantage of inefficiencies in the people themselves and some loopholes in the law.

The simplest business fraud is the fake invoice. This piece of idiocy should never work, but it does often enough to make it worthwhile. The fraud artist makes up a company name and establishes a bank account in that name. He orders invoices printed, picks up the Yellow Pages, and sends invoices for nonexistent deliveries and services to the companies he culls from the directory.

Theoretically, this should never work. In companies which have even a rudimentary accounting system, staffed by conscientious people, it doesn't. Each delivery or service call is documented, with a receiving ticket written up and stapled to the packing slip or service slip, a copy of the ticket going to the person authorizing the purchase and another to accounting, where a clerk vouches it against the original purchase order. The purchase order is the key, and companies which have, and enforce, a strict rule that every procurement must have a purchase order signed by the individual authorized to do so, will not be vulnerable to this scam.

Often, however, especially in small companies, there is no system, and it's impossible to tell from any available paperwork which are legitimate invoices and which are bogus ones. A harried, overworked clerk issues a check and passes it on to the executive whose signature is authorized. Often, the executive will sign anything he finds before him, assuming that if the check is already made out it must be legitimate. This lack of internal controls leaves the company wide open to the fake invoice.¹

A step up from the fake invoice is the fake service call. This ploy takes advantage of the fact that even in well-run companies, service calls often don't have purchase orders to authorize them, or else have a "blanket purchase order" issued to cover them. American business, like the Government, is flooded with

paperwork and the blanket purchase order or other informal arrangement is an attempt to reduce the paperwork load by eliminating the formality of a purchase order for routine items. Moreover, authorization of a service call does not usually go through the usual channels, with a written requisition passed to the purchasing agent, who then arranges for the work to be ordered. A typist may contact the typewriter repair company for a service call, without being required to clear it with the purchasing agent, the comptroller, or any other executive.

The con man, armed with a pad of service call tickets, arrives at the office and tells the receptionist that he's there to service the typewriter, for example. The receptionist, upon checking with other people in the office, finds nobody who called for service. The "service man" then requests that the receptionist sign a service ticket, purely as a formality so that he could justify his time to his supervisor. He hands her a carbon of the ticket, and leaves.

The ticket is also an invoice, and some days later a copy arrives in the mail. Printed on it is a minimum charge, which applies whether there is any work performed or not. If the accounting clerk phones to question the invoice, the con man, who has established an office or who works out of his home, answers that someone made a service call and he has a signature on his ticket to document it.² Of course, the matter would not stand up to close investigation, but as the amount on the invoice is usually small, there rarely is any follow-up and the company usually pays.

A more involved business fraud is called the "bust-out." Although simple in principle it is difficult to execute, and often takes weeks or months to carry out. The first point is for the con man to acquire control of a business, which can come about in a number of ways. A businessman who has a weakness for gambling, for example, is open to having a con man take control of his company to settle a large debt. Another way is to buy an existing company on a short term loan. The key is the company must have either a large inventory or an excellent credit rating. If there is a loan involved in the buyout, selling the inventory at cut-rate prices will raise the money to pay off the loan. Otherwise, the company's credit rating is helpful in acquiring a large quantity of merchandise to sell off quickly.

Basically, the system of profiting from a bust-out is to use the company to purchase as much stock of goods as the creditors will allow, selling it quickly, and then either leaving town or declaring bankruptcy.³

In the "bust-out" there is usually a front man, called a "pencil," an honest executive who is not in on the fraud. He is the one who runs the routine operations of the company while the fraud artist concentrates his efforts on the scam. The "pencil" is also the one whose feet will be in the fire after the fraud artist leaves town and he'll have a hard time proving he was not party to the scheme.

The mechanics of a bust-out can be very elaborate, depending on the imagination and resources of the con man. If organized crime is involved, there will be a group of "legitimate" companies taking part.

One of the myths of the Twentieth Century is that those involved in organized crime sometimes decide to "go straight," investing their criminal proceeds in "legitimate" business. In reality, they establish a "legitimate" source of income to satisfy the IRS, for laundering money, and as receivers of illegitimate goods.

Such a company can buy goods sold at a low price during a bust-out and resell them at a large profit. In fact, a fraud artist who is connected with organized crime can use a bust-out to supply his "legitimate" company at very low prices, enabling it to beat the competition.

The end of the game can come two ways: The con man can simply leave town after having extracted as much as he could from the purchase and quick sales of inventory. The appropriate moment is when the vendors are unwilling to supply any more goods on credit and begin pressing for payment of the debts.

The other way is to declare bankruptcy. To support this, it's necessary to have the proper invoices, bills of sale, and other paperwork to support the transactions, as the bankruptcy court will be interested in the events that led to the bankruptcy. There are several ingenious means of disposing of the money, and their success depends on the imagination of the con man, as well as on luck.

NOTES

1. *Classic Mail Frauds*, Scot Tinker, Eden Press, 1977, p. 12.
2. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, pp. 27-28.
3. *Big Time Operator's Manual*, Scot Tinker, Eden Press, 1977, p. 14, pp. 38-39.

CHAIN LETTERS AND PYRAMIDS

Almost everyone has gotten a chain letter at one time. The chain letter urges the reader to send a dollar, or some other sum of money, to the name at the top of a list, then retype the letter, deleting the top name and adding his own at the bottom. The letter promises riches to the people who follow the plan. As Carey and Sherman so carefully calculate in their book,¹ the chain soon snowballs to involve a fantastic number of people, and only the originators of the chain letter stand a decent chance of making any money.

The principle of the chain letter is that of the pyramid, with a small top and large base. All money flows towards the top, and the people on the bottom, in reality, are the payors, not the collectors.

As we shall see, there are many fraud schemes built upon the principle of the pyramid. Referral sales schemes, in which the buyer hears that he'll get his water softener or other merchandise free if he steers enough of his friends to the salesman, are a good example.

Another is pyramid sales, in which the major effort is to build up a network of "dealers," rather than selling the goods to the public. As in all pyramid schemes, the bubble eventually bursts because there are only a certain number of people and the scheme, which depends on continued growth, collapses when the limit is reached.

NOTES

1. *A Compendium of Bunk*, Carey and Sherman 1976, Charles C. Thomas. pp. 48-55.

DOOR TO DOOR

There are legitimate door to door sales companies, among them **Fuller Brush and Avon**. There are also many sleazy, fly-by-night outfits that peddle fraud.

For years, legitimate street salesmen have sold their goods to householders in a more or less honest manner. While some of them did practice dishonesty, most of those representing a legitimate company gave the customers what they purchased. The prices were somewhat higher than prices for similar items in stores because of the commission system. Most people aren't aware that street salesmen earn from twenty five to fifty percent commissions.

There were some instances of fakers impersonating salesmen for reputable companies, taking orders and accepting deposits, and never returning. Most fraud artists, however, were interested in more than the small "take" from this sort of operation.

In the small league there are also those who go from door to door pretending to be collecting money for one charity or another. Sometimes the charity does not exist, other times the charity is real, and the credentials stolen, or forged.

All of these street salesmen (and women, too!) first have to get the victim to open the door. Sometimes the enticement is a "free gift," and at other times it is the offer of a "free" demonstration. The salesman may elicit sympathy by stating that he gets paid for just giving demonstrations, which is an outright lie. Sometimes, the salesman will tell his intended victim that he'll qualify for a discount if he allows him to make a demonstration. This, too, is part of the con.¹

There are several tired old schemes for selling goods door to door, but new ones pop up every year. The old vacuum cleaner pitch, in which the salesman dumps a bag of dust and sweepings on the floor at the first opportunity, then comes in and cleans up the mess with the new vacuum cleaner, has been done very often, and it's still offensive.

Often, as in freezer food plans, there is a deceptive pitch regarding the money to be saved by buying frozen food with the

plan offered. The plan involves, of course, buying a freezer at an inflated price. As this is the object of the whole exercise, the salesman tells the customer that he can drop out of the plan at any time he becomes dissatisfied. He glosses over the point that the customer is stuck for the freezer. Many customers do drop out when they find they are not getting lower food prices with the plan.

Another piece of hardware that keeps selling is the water softener, especially in areas of the country that have hard water. The salesman, often with an appointment made for him by a "boiler room" operation, arrives and launches into an hour long pitch regarding the perils of untreated water. He'll open up a large case containing laboratory glassware and vials of chemicals, and "prove" to the homeowner that he's ruining his plumbing and risking his health by allowing untreated water to flow through his pipes. There may be some special enticements, such as an "introductory discount," or a referral plan to allow him to get his water softener free by steering the salesman to his friends, but in the end the victim signs a contract for a water softener at a price higher than he would have paid at a local store. Add to this installation charges which are also inflated, and the cost of a credit contract, and the homeowner spends as much as fifteen hundred dollars for something which would cost him three locally.

Water softener salesman hand out "lifetime" guarantees, knowing they won't honor them, as the "company" will fold its tent and move on shortly.

Such salesmen tend to push trendy items, closely following the fads in the media. For the last few years, "solar" and other energy saving devices have been pushed hard. Twenty years ago, the trend was nuclear bomb shelters and allied equipment. Many backyard "contractors" set themselves up as "experts" on shelters, just as today out-of-work plumbers put together simple and cheap arrays of pipes and tanks and sell them as "solar" water heaters, promising the homeowner will recuperate the inflated prices quickly through savings on his utility bills, a claim which is impossible to check out until it's too late.

There is now some protection for the victim of an unscrupulous salesman. Some states have laws providing for a "cooling off

period.” usually several days, during which the buyer can think over the contract he signed and, if he changes his mind, annul it by notifying the company.

Some salesmen still use the blank contract trick, offering the customer a blank form to sign and telling him that he'll fill it in later, at the office. The excuses for this vary, but they still work on people who are not careful.

It's in the field of home improvements and repairs that the con artists really hit hard. Some of them even impersonate public officials, such as building “inspectors.” One group passed themselves off as “termite inspectors” for the city, and inveigled victims into paying for the extermination of termites that were allegedly infesting their homes.²

A particularly brazen duo claimed to be gas company repairmen trying to trace a “gas leak.” They rang the bell and asked for permission to enter the yard to check the pipes. Starting a small fire, they quickly put it out and told the householder that the house was unsafe for occupancy. While in the house, they stole a wallet and some money that had been in a hiding place in the refrigerator.³

Fake “inspectors” have persuaded many homeowners they needed work on their septic tanks, roofs, plumbing, wiring and heating systems. One bold scam was the “furnace inspector” who gained access to the house on the pretense of “inspecting” the furnace. After disassembling the furnace, he told the homeowner it was in a dangerous condition, and that he suggested buying a new furnace. Of course, he was willing to suggest from whom he should buy it. If the householder refused to buy a new furnace, the “inspector” left the old one in pieces on the floor of the basement.

The “inspector” ploy is very effective if the victim is not too bright, and credulous when the “inspector” reinforces his sales pitch with the threat of a fine. With the threat of a large fine hanging over him, the homeowner is relieved when the “inspector” tells him that if he gets the defect fixed immediately, he won't report it. By coincidence, the “inspector” has a friend in the business who can perform an immediate repair. This ploy works

especially among sophisticated city people, because they are so accustomed to “shakedowns” by public officials they are relieved this “inspector” does not ask for a bribe, but on the contrary seems to be going out of his way to be helpful.⁴

Fraudulent roof repairs and driveway blacktopping are still with us. One variation used is the “leftover” ploy. The workman rings the bell and informs whomever answers that he just finished a job down the street and has enough material left over to “waterproof” the roof or driveway. To avoid the nuisance of hauling it back to the yard, he’ll let the homeowner have it for far less than he’d normally pay. The price is right, but the material is cheap, often being just used motor oil for the driveway blacktopping. The workman collects his money, and when the first rain comes the oil washes off.⁵

A big ticket item in home repairs is the aluminum siding fraud. The sales pitch can be very high-pressure, with the salesman claiming to have a “special introductory offer” to push him into signing. Some will use the referral sales pitch, telling the victim that he’ll get a certain amount back from each additional sale if he allows his house to be used as a “demonstrator.” In some extreme cases, the salesman will tell the customer, if the price seems to be more than he can afford, that he’ll lend him the money for the initial payment out of his own pocket to get the order. He then has the customer sign a credit contract, which makes it a three-party deal and enables the salesman to collect his money immediately and earn a commission on the contract from the credit company, and leaves the householder with long-term payments.

Similar tactics prevail in sales of other home “improvements,” such as swimming pools and remodeling projects. Although the work may be honest, and the materials sound, the sales tactics tend to be high-pressure, and often cross over the line into fraud.

NOTES

1. *Fraud Investigation*, Glick and Newsom, Charles C. Thomas, 1974.

2. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, p. 8.
3. *A Compendium of Bunk*, Carey and Sherman, Charles C. Thomas, 1976, p. 60.
4. *Clipping The Flocks*, pp. 8-11. *Compendium*, p. 42.
5. *Clipping The Flocks*, p. 12.

DRUG “BURNS”

Keeping in mind the ease and enthusiasm with which fraud artists prey on ordinary citizens, it is not surprising they also prey on each other. One extremely profitable, and extremely dangerous, way in which they do this is in narcotics deals. When a supplier of a contraband drug offers to supply a dealer or a wholesaler with a large amount, the opportunity to make a large profit very quickly exists, and the opportunity to make an even larger one by supplying a worthless substitute is tempting.

This practice has become so common that a special term for it exists in our language, the “drug burn.” “Burning” a buyer by substituting lactose or talcum powder for heroin, for example, is one way in which the seller can attempt to cheat the buyer. Another is by excessive dilution.

It is an old saying that there is honor among thieves, but this widely accepted dictum is almost always false. Those who prey on the public have no inhibitions about preying on each other, if the opportunity exists and if they think they can succeed. On drug deals, there are roughly two types of “burns.”

The first is to substitute a counterfeit substance for the drug. This is why large contraband drug dealers now use chemical tests to assay the authenticity or purity of the substance at the time of the buy. There are available small and portable test kits, usually sold to police, for this purpose. While these were originally conceived for the use of drug enforcement squads, the companies who make them are under no legal requirement to sell them only to police agencies, and many of them find their way into the hands of drug dealers and wholesalers.

The larger dealers, who buy quantities worth hundreds of thousands of dollars at a time, often employ their own chemists, who come to the site of the exchange and test the questioned substance on the spot.

The other variant is the outright “ripoff,” in which the dealer or distributor attempts to take possession of the drug without paying for it. This crosses the line between fraud and robbery.

The prospect of suffering huge losses in dishonest deals results in the participants in illegal drug buys coming armed, and often a shootout occurs when the deal “goes down.” This accounts for a certain proportion of the corpses that turn up shot to death with no witnesses. Such murders are difficult to solve, as the connection between the victim and his killer is clandestine.

On a smaller scale, the dealer often attempts to cheat his addict clientele by diluting the drug beyond the usual amount. He knows the addict lacks the recourse that the victim in other frauds has, that of reporting him to the police.

Without getting too far afield, it is worth noting that “burns” and “ripoffs” occur in other illegal transactions, such as “fencing” stolen goods, and that contraband is not limited to controlled drugs, but also includes currency, gold, diamonds, and other smuggled items. These transactions can also lead to violence, but much more rarely than those involving drugs.

ENTRAPMENT

Any involvement with sex or romance offers the fraud artist an opportunity to defraud a victim. Lonely hearts clubs and Murphy **men victimize lonely people. For the most direct and blatant fraud,** falling short only of an actual hold-up, the “badger game” stands out.

In its prototypical form, the badger game requires a man and a woman working in concert. The woman allows herself to be “picked up” by a man. Any man will do, but if he’s a married man on a business trip, seeking a little excitement outside his marital relationship, he’s a prime candidate.

After the pick-up, the couple goes to the woman’s lodging. When they’re comfortably and compromisingly between the sheets, the male partner of the fraud duo comes in, pretending to be the woman’s husband. Quite expectedly, a row ensues, with the “husband” angrily denouncing both his “wife” and her lover. During the discussion, the “husband” threatens to notify the police, or the John’s wife, further raising the level of anxiety. This sets the stage for a “settlement.” Sometimes prompted by the “wife,” the mark offers the husband money to soothe his hurt feelings. If the mark is lucky, that’s the end of it.¹

There are several variants on this scheme. If the mark is married, he’s very open to blackmail, and the payments may last a long time and involve a large sum of money. Another angle is the compromising letters variant, in which no physical contact need take place and which can be run by one man. The con artist places ads in lonely hearts and “swinger’s” publications, claiming to be a single woman seeking a good time. When the replies come in, he answers in an enticing manner, and sooner or later collects some letters from married men who have been foolish enough to put their desires for illicit relationships on paper. Depending on his resourcefulness, the con artist can trace some of these potential victims, even if they use post office boxes for their contacts. At this point, he can pretend to be either an outraged husband who has discovered his “wife’s” compromising mail, or an outright

blackmailer, who threatens to show the letters to the victim's wife unless he pays him for silence.

Another variant is for one or more men to burst into the room when the couple is in a compromising position, pretending to be police or private detectives. This variant works when the couple go to a hotel, where it is unlikely that the "husband" would have a key to the premises. The "private detectives" claim that they have been **hired by the woman's husband, and they may even take photographs upon entry.**

If they claim to be the police, they may claim to be from the vice squad, enforcing the law against illicit sex. There may or may not be an applicable law in the state in which a particular badger game runs, but if the victim is from out of state he will be unaware of this. In fact, some states still have archaic laws pertaining to sexual conduct.

Yet another variant on this scheme is the "underage girl" ploy. This requires that the fraud artist work in concert with a teenage girl who looks older than she is. The "police detective" bursts into the room and threatens to arrest the mark for relations with a minor. The girl tearfully reveals that she is under the age of consent, and the stage is set for extortion.

Yet another tactic is for the female partner in this game to be of legal age, but able to pass for younger. If the "pickup" occurs in a bar, the mark will assume that she's old enough, as operators of bars are forbidden to serve alcohol to minors and usually are careful in checking customer's ages. When the "detective" bursts in, he claims the lady's driver's license or other proof of age is forged, or stolen, and that she's really a minor. As sexual relations with a minor is a felony in all states, often falling under the law regarding child molesting, the mark has good cause to worry.

A variant about which we hear little is the homosexual one. Most states have laws pertaining to "unnatural acts," "crimes against nature," or "sodomy," and although these are not usually enforced when the relationship involves consenting adults, they are still on the books and ready for use when the act takes place outside a private home or apartment.

The victim may be either an overt homosexual or a married man with a secret life who indulges when away from home. While the married man has the most to fear, since he usually does not want this dark side of his personality revealed to his wife or employer, it's a mistake to assume that the hardened homosexual is invulnerable.

Sexual relations with a minor are also illegal when the contact is homosexual, and the man who picks up a male who later turns out to be "underage" is open to felony prosecution. Because of the highly emotional nature of popular attitudes towards sexual misconduct, and especially sex with a minor, penalties are likely to be severe. Combine that with homosexuality and we have a truly threatening combination.

The fake rape is another variation of the badger theme. The "rape" can be statutory or violent. In its simplest form, it doesn't even require more than the female, who allows herself to be picked up. In the car, or in the room, she tears her clothing, dishevels her hair, and claims that she'll call the police and charge the mark with rape, unless he pays her. She may play the role of a casual pickup, and then demand money, or she may play the outright prostitute and demand, instead of the agreed fee for service, the entire contents of the victim's wallet.²

She may, after consummation of the act, claim to be underage, and demand payment in return for silence. It's obvious that this theme can have both hetero- and homosexual versions. Whatever the form, the badger game, calculated to cause the victim to panic, works very well and fraud artists who play the badger game find new victims for this old trick every day.

NOTES

1. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, p. 15.
2. A fellow employee of the author, when both were working the police beat for a newspaper, picked up a young lady who was hitchhiking. Shortly after she entered the car, she tore her clothing and informed the driver that she was going to scream "rape." The

driver had good presence of mind, and pulled into the parking lot of the police station, which was nearby, and told her to scream all she wished. He explained to her that he was acquainted with most of the members of the police force, and that the likely result was that she would be arrested. This is a rare example of total failure of the badger game, caused by a combination of a cool and calculating mind and good fortune. Most intended victims don't fare as well.

It doesn't always end so well. Sometimes, the victim can't go to the police because the fraud artist is the police. There is a small minority of crooked cops who "shake down" their victims, threatening them with arrest unless they pay up. This happens mainly in vice and gambling investigations. However, in some of the better-run police departments, there is hope for the courageous victim, if he reports the incident to the "internal affairs" department, which is the section of the police that polices the policemen. They investigate the alleged wrongdoing, and the result is not always a whitewash.

FLEECING RELATIVES

In some con games, the victim is not the target, but a relative or neighbor, or even a friend, is. The target is merely the lever the con man uses to pry money loose from the victim.

One simple con is the "dead man's debt." Scanning the obituaries, the con man works up a list of recently deceased people and the addresses of their survivors. He approaches the relatives, claiming that the deceased had borrowed money from him but died before he could repay the loan. Although this con is old, it still works.

A variant on this is the C.O.D. racket. The con artist, posing as a delivery man, brings a package to the widow, son, or other survivor at the same address as the deceased. He claims the deceased had ordered the goods. Acting surprised and sympathetic, he collects the money and runs.

The C.O.D. racket also works with living persons. The phoney delivery man brings a package when the addressee is not home, and leaves it with the wife, other relative, or even a neighbor, of course collecting the C.O.D. charge.

Modern technology makes it possible for the con man to work some variants of this racket at long distance. One type who victimizes people by remote control is called the "sheet writer." He works by frequenting hotels and resorts, striking up conversations with guests. Whether tourists or conventioners, they are vulnerable to the sheet writer, who during the course of the conversation asks many friendly and seemingly harmless questions. He'll ask if the victim is married, the names of his wife and children, and many other details in a manner which will not seem probing but will flesh out the frame of the acquaintance. His manner will be flattering and friendly, and perhaps he'll reveal that his home is not too far from his target's. In parting, he'll of course ask for his target's name and address, promising to phone or visit when he returns home.

Armed with this information, he wires the target's wife or business associate. Tersely, the telegram explains that he lost all of

his money through a mishap, mentions some personal details to authenticate the request (your middle name is Helen, your mother lives in Council Bluffs) and asks for additional funds to be wired.

The basis of this trick is that the target supposedly lost his wallet, and therefore cannot supply official documentation to identify himself, as is normal procedure when receiving "Moneygrams." He asks that the sender instruct the telegraph company to require the collector of the money to give a piece of personal information, which he already knows from requesting the target. This enables the con man to collect and cash the wired check without proper I.D.¹

There are many variants on this basic ploy. The con man may not always pose as a friendly acquaintance, but instead identify himself as a writer doing a story on the convention, a public relations executive for the hotel, etc. This semi-official role-playing will often open up people who otherwise would not be inclined to be friendly and discuss themselves. Again, without seeming to probe, he elicits personal details. Among the important details are the name and address of the nearest relative, or the business associate, along with the phone number.

Choosing a moment when the target is away from the hotel, in case the relative decides to check by telephoning, the con man rings the number. He explains that he's a bail bondsman, that the target has been arrested on a relatively minor charge, and that he needs several hundred dollars to arrange bail. The con man adds that the target told him to mention some personal details, such as the names of the children or pets, to indicate that the request is authentic.²

This maneuver enables the con man to receive payment under his own identity, or any for which he has official documentation. Using this technique, he can collect several thousands of dollars in one day or evening.

NOTES

1. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, P.O. Box

8410. Fountain Valley, CA 92708. p. 31. Also, *Short Cons*, Scot Tinker, Eden Press, p. 9.

2. *Short Cons*, p. 28.

GAMBLING DANGERS

Gambling is an interesting pastime for some, an addiction for others. It's a way for some to earn a lot of money quickly, and to lose a lot quickly for others.

Gambling among equals has its hazards. Luck can cause one to win, and the other to lose, sometimes quite heavily. This is normal, and it's obvious that gambling for more than an affordable amount is poor practice. A "friendly" game can turn into a disaster.

Gambling in a commercial, above-board gambling establishment has its problems, too. Obviously, a racetrack or a casino is set up to earn money, and the odds always favor the house. For example, the games in a casino pay off at slightly less than true odds, so the casino gets its six percent (usually) "off the top." At a race track, the parimutuel system is set up so that in effect the players are betting against each other, not the track. The payoffs are always less than the amount of money wagered and the track takes its fee off the top before paying off. The commercial establishments are usually honest, in the sense that the odds and payoffs are known to the players, and there are security precautions against cheating either by players or dishonest employees. This is necessary because any suspicion of dishonest practice can damage the reputation of a casino or track, and reduce business. Commercial gambling establishments are also monitored by a government agency, usually a state gambling or racetrack commission, to insure further the honesty of the transactions.

For the individual gambler, the summing-up is that, in honest games with friends, he should break about even in the long run, assuming a normal amount of luck. In playing at commercial establishments, he will lose over the long haul, because the house skims its profit off the top, before assigning payoffs. The games against professional gamblers, however, are another story.

Professional gamblers are a little documented subculture in our country. There is much misinformation about them, and few facts

available to the public. There is a myth that some of them are extremely sharp and perceptive players, who by superior skill manage to earn their livings at cards, dice or whatever game they play. It's a safe assumption that there are very few of these, just as there are very few outstanding people in any field.

In reality, the people who earn their livings at gambling do so by cheating, as in any other con game. They are fraud artists, in addition to breaking the law in other respects in states where gambling is illegal.

In some states, the law comes down very hard on gamblers whether honest or not. There have been some instances of church bingo parties running into difficulties with the police. The effect of these laws is usually counterproductive. The laws keep gamblers underground, and they discourage those who have been cheated from complaining to the police because that involves a confession that they were participating in an illegal activity.

Some gambling fraud operators are truly freelance, working alone and depending on their skill at cheating to stack the odds in their favor. More often, however, they work with confederates, who aid in "steering" business their way rather than in the fraud itself.

The classic card swindle is called "three-card monte," and usually works in this manner:

The "game" takes place in an area accessible to the public, where the mark comes across an old man playing with a younger one. The old man shuffles three cards and places them face down. The younger man has to pick the red card from the three. Each try has some money on the table to cover the bet. The younger man picks the correct card every time, which is not surprising, because the corner of the red one is slightly bent. If the mark bites, when he tries to pick the red card he fails every time, because the old man, who's part of the scheme, has switched a black card with a bent corner for the red one.¹

In this game, the old man may pretend to be drunk, to aid the illusion of incompetence. The younger man is a shill. There may be a third party, seemingly unconnected with the game, to "steer" the victim to the game.

Marked cards are common devices used in cheating. Originally, individual cheaters marked the decks themselves, but in the Twentieth Century marked decks have been manufactured. They are available in novelty shops in many large cities.²

Playing dice, or "craps" is a daily activity in many communities. If the players know each other, there may be no cheating. However, "loaded" dice have been around for years. These are dice which are weighted, or have rounded edges or other alterations resulting in one side or one set of numbers coming up more often than another.³

Playing with coins betting on the fall of heads or tails, can also be a fraud. Cheats modify their coins by chamfering the edges so that they fall on one side more often than the other.⁴

All told, fraud systems and devices are very common in gambling. Gambling with friends is hazardous enough, but gambling with strangers is a sucker's game, indeed.

NOTES

1. *Short Cons*, Scot Tinker, Eden Press, 1977, pp. 9-10.
2. *The Bunko Book*, Walter B. Gibson, 1976, Gambler's Book Club, pp. 50-58.
3. *Ibid.*, pp. 41-49.
4. *Ibid.*, p. 58.

HEALTH CARE FRAUD

The success of health care frauds provides a conspicuous exception to the widely-held belief that "you can't cheat an honest man." The victim is not seeking treatment out of greed, or in the hope of getting something for nothing.

This field is extraordinarily complicated, and we shall see that frauds are perpetrated by licensed medical men as well as "fly-by-night" types. We shall also see that in some instances fraud artists are protected by law, incredible as it might seem.

Let's start our survey with some obvious frauds. It's well known and widely accepted that a doctor must see his patient in person in order to examine him and prescribe proper treatment. Yet, in Tampa, Florida, a licensed physician was convicted of treating patients by mail order.¹ The physician involved had a degree in osteopathy, not an M.D., but osteopaths are recognized and licensed in most states, and their training is as comprehensive as that of M.D.s.

Another type of medical fraud is practicing medicine without a license. It is impossible to ascertain the number of bogus doctors in this country because detecting a fake is very difficult in practice. There have been a number of spectacular imposters who have played doctor, sometimes for years.

Typically, the way they do it is to assume the identity of a real doctor. While a fake diploma from a non-existent medical school may fool a patient, a hospital administrator will be more sophisticated and recognize it immediately as a fake. In the cases which have come to light, the imposter presented impeccable credentials in the name of a real graduate. It is standard practice to send for the transcripts of the records, and these did check out. In the cases in which the bogus doctors were exposed, it came about that another member of the staff had been to the same medical school at the same time, and did not remember the imposter. It is obvious that, with the large numbers of medical directories available, the employer did not do his homework. If a person presents himself as being "Dr. George Smith," it is not only

possible to verify his medical school and licensing records, but it's easy to check the name in the Directory of Medical Specialists or the American Medical Association listing. It's also easy to check with the local medical association from the locale the applicant claims origin.

It is a difficult task for the patient to check out his physician. He does not have the time or investigative resources to do so, and usually does not even know how. There have been instances in which even a government agency has been slow to react. A bogus "Doctor" of psychology applied for, and got, a job as chief psychologist at the state prison of one of the smaller states. He held this position for almost a year before the administrators completed their investigation and found that his qualifications were false. During this time, he expanded his horizons. In collaboration with a former inmate of the prison, a man convicted of fraud and paroled after serving nineteen months, the bogus psychologist took to spending time at a local exclusive (high priced) resort, where he did his best to make the acquaintance of wealthy people. In one instance, he became acquainted with a very wealthy local auto dealer who was having problems with his marriage, and undertook to "counsel" him at the rate of fifty dollars an hour, which was a substantial fee at the time, 1970.² Meanwhile, the psychologist had defaulted on payments on a rented car, and stood off the agents who came to reclaim it by telling them they had no authority on state property, where he lived. **The prison provided its officers with living accommodations on campus as it were, with security provided by the guard force.**

This "psychologist" had the usual impressive credentials, including expensively printed diplomas. Few people realize that diploma blanks with decorative borders are stock items with printers, and that most printers will print anything the customer wants without question, except for obviously illegal counterfeiting of U.S. currency.³

Finally, the "psychologist's" bogus past caught up with him, and the prison authorities informed him that he could no longer continue in their employ. Strangely, they did not arrest or prosecute him, but merely gave him ten days to pack up his

belongings and move out of the house which they had provided. He drifted to another state, where he had previously been charged with using the title "Doctor" without a license, and took up other scams to earn his living.

For many decades, the American Medical Association has acted to require strict licensing requirements for physicians, in an effort to drive out the quacks who get their diplomas from diploma mills or print them outright. They have been successful, in that many outright quacks have been put out of business, but it's important to note that there is also an element of self-interest at work. Often portrayed as the most powerful union in the nation, the AMA has been very protective of doctor's privileges. Recently, it took to the U.S. Supreme Court a case in which a local medical society was accused of price fixing, claiming that establishing prices for services rendered should be exempted from the law that applies to other businessmen. The Court decided against the AMA in this one.

The AMA takes very seriously any doctor who attempts to undercut the prices of his colleagues. In other fields, providing better service at lower cost is common practice, but not in medicine.

It's also worth noting that doctors often own stock in hospitals, which brings up the question of conflict of interest. Hospital costs have been in the headlines very much lately, with doctors claiming that hospitals are jacking up prices beyond all reason. Yet they continue to send their patients to hospitals without checking to determine which ones offer the lowest prices. They continue to admit patients to hospitals for procedures that require only office surgery or treatment in outpatient centers.

A good example is the doctors' attacks on the home birth movement. Doctors are almost unanimous in their contention that home birth involves risk if there are complications, and the home birth practitioners point out that until the Twentieth Century, most babies were born at home, and in many parts of the world still are. They say that it is possible to take care of high-risk pregnancies in a hospital, and have the rest delivered at home. Doctors, of course, see their income threatened by this, and

oppose it bitterly, saying that only hospitalization can cope with the risks of pregnancy and birth, failing to point out that the United States, with its abundance of hospitals, does *not* have the lowest infant mortality rate in the world, which we would expect from this level of care. In one instance, a local hospital threatened to revoke the privileges of one doctor who delivered his patients' babies at home.

The AMA has had a running gunfight with alternate health care practitioners for decades, throwing them in with the quacks, and maintaining the position that nobody except a graduate of an AMA-approved medical school can be competent to care for patients. Chiropractors, for example, have been on the receiving end of an unrelenting attack, despite the fact that there are many people who have been helped by chiropractic.

Medical doctors claim a patient may suffer because he may have a serious illness that the chiropractor is not competent to diagnose and treat. There is another side to this coin. One man, for example, had been suffering from tension headaches resulting from stress on the job. His medical doctor had prescribed a tranquilizer, which turned out to be ineffective in coping with the headaches and left him with a groggy, dozey feeling that impaired his effectiveness on the job. Against his better judgement, because he had little faith in chiropractors, he consulted one. He had immediate relief from his headaches.⁴

The central fact about alternate health care is that the issues are not clear cut. First, established medicine is not completely aboveboard. Licensed physicians continue to prescribe unneeded treatments and unnecessary surgery to line their pockets.

Unnecessary operations are known in medical jargon as "renumer ectomies," and their occurrence is so well known as not to require further discussion here.

Another unethical surgical practice is known as "ghost surgery," in which the surgeon who actually performs the operation is not the one whom the patient has been seeing, but a lower paid resident or intern. This enables the surgeon who subcontracts the work to handle a heavier caseload, collect full-size fees, and make a profit on each operation after paying the "ghost."

Thus we see that even licensed medical doctors are not all totally honest. Whether they are competent is another question, and an important one because the medical establishment claims that those who are not M.D.s are bad because they are not capable of treating patients.

Doctors make mistakes, some more than others. Yet, they are very reluctant to admit this. It is dirty linen which they do not air in public view. Most of us have had the experience of an illness which a doctor was not able to treat successfully, or have had relatives who were unsuccessfully treated by an M.D. We also see, in reading medical journals, wheedling phrases such as "the patient did not respond to therapy" or "...the patient's progress was disappointing..." which imply that it was the patient's and not the doctor's fault that he did not do well. Granted that there are uncertainties in medicine, when we get to how the doctor collects his fee we can see how differently he performs from other people who provide services. The doctor presents his bill whatever the outcome. We do not expect this from those in other occupations. We don't expect to pay a mechanic if he doesn't solve the problem with the car. Moreover, reputable mechanics warranty their work. If, after payment, the problem still exists or recurs, we return the car and expect satisfaction.

Non-performance by auto mechanics, plumbers, carpenters and electricians can result in complaints to the Better Business Bureau, and cases in small claims court. Non-performance is breach of contract. When a major corporation, for example, fails to perform properly the work it contracts with the Defense Department, the result is sometimes a lawsuit involving a substantial amount of money, as in the instance of National Semiconductor recently.⁵

Other parts of the medical establishment require a close look. The "ethical" drug companies have for years sold prescription and non-prescription drugs that were ineffective. Over the last few years, action by the Food and Drug Administration has forced the withdrawal of ineffective drugs, and one of the standards for new drugs is that they must do what they're supposed to do. The burden of proof is now on the drug company seeking to market the

new drug, and it must submit to the FDA proof of effectiveness as well as proof of safety for use in humans.

The standards are still lax, and we find on the shelves many preparations with supposed medicinal value that actually do not work. The profusion of diet pills is a good example. None of these cause weight loss, and the leaflet that comes in the package usually provides a diet which the user must follow. It's clear that following the diet causes the weight reduction, not the ingredients of the pills.

Diet preparations are only part of the problem. There are innumerable others cleverly advertised to attract buyers without making claims that are in flagrant violation of the law. Baldness cures, complexion products, and others that fall into the category of cosmetics follow the same pattern.

They are all overpriced. Few buyers know the margin of profit involved. A preparation that contains petroleum jelly, lanolin, a weak concentration of a vitamin, and scent often sells for several dollars. It costs just a few cents to manufacture, and is usually a standard formula, not a "new beauty secret" as claimed.

It is still legal to produce and sell ineffective preparations, providing that the seller avoids infringing the weak laws governing them. There are many loopholes, and the largest companies employ staffs of lawyers who work to find and exploit these loopholes.

Turning to the outright illegal efforts which have been successfully prosecuted, we start with the case of two chiropractors who treated cancer, epilepsy, and other serious illnesses with a machine of their own invention. They also offered a diagnostic service by mail-order, at fifty bucks a throw. As part of its investigation, the California Department of Public Health had an agent send blood samples from a sheep, a pig, and a turkey to the "diagnostic laboratory." The diagnoses offered were chicken-pox and mumps.⁶

The field of cancer cures is very lucrative, with both real and bogus practitioners selling drugs that have proven ineffective. Often, they claim the medical establishment is conspiring to

suppress their discoveries because a real cancer cure would mean a loss of income for doctors. This has a core of truth, and people who have had disappointing experiences with greedy doctors find it easier to accept.

The bedside manners of “real” M.D.s do not build confidence. Many of them are arrogant and brusque, and it is general practice for them to keep patients waiting for their appointments and then process them in a manner like that of a supermarket checkout.⁷

By contrast, the bogus drug sellers and other fake practitioners have kindly, sympathetic approaches. They are masters at winning people over. They are con men. This is the real reason for their continuing successes.

A formerly licensed physician distributed “liefcort,” a valueless drug, by mail-order.⁸ “Krebiozen” is another, more widely publicized drug which has turned out to be worthless but which has earned large sums for its distributors.⁹ A recent effort was the promotion of “Laetrile”, a supposed cure for cancer. While many people claim to have been helped by Laetrile, it has been banned in the United States.¹⁰ It is now being offered to cancer sufferers in Mexican border towns, where Americans come for treatments.¹¹

As we’ve seen, one reason that people choose to try some of the bogus artists is their experiences with M.D.s have been unpleasant. Another is that conventional medical treatment has failed. Conventional medicine has failed to find a cure for arthritis, a chronic illness which, although not usually fatal, is so painful in some cases that the patient might well wish it were. A cancer patient who has spent much money on conventional doctors may feel that, with his life at stake, he’ll try anything, as he has nothing to lose. While the quack may truly be incompetent, licensed physicians also misdiagnose cases and prescribe the wrong treatment.¹² To the patient who is desperate, any hope is worth following up and grasping.

Some of the medical frauds are outlandish. They involve bizarre machines and procedures, and promise “miracle” cures. One scam had the victims sitting in worked-out uranium mines where the radioactivity had supposed curative powers.¹³ Another sold copper

bracelets as cures for arthritis. Some are in the weight-reducing business.

On the fringes of health care are many others, such as naturopaths, homeopaths, hypnotists, and various “counselors.” It would be wrong to label all of these quacks, as the scientific foundation proving or disproving the value of their work is by no means clear. There are no clear-cut rules of thumb to distinguish the quack from the legitimate practitioner.

If we judge a con man by his smooth and considerate manner, we must admit there are doctors who show much consideration for their patients.

If we look for bizarre equipment that works according to arcane principles, we’ll find it hard to distinguish a CAT scanner from an orgone box without specialized and technical knowledge.

If we judge by results, it will be difficult to decide if successful or unsuccessful cases are good indices of the worth of a treatment. While the surgeons who performed heart transplants developed international reputations, most of their patients died. The widely-publicized artificial heart has not been an outstanding success, to say the least. Doctors still can’t cure colds. This confusing picture points up how truly difficult it is to spot a “quack.”

What complicates the picture even more is that some of these disapproved cures *work*. Hypnotists, for example, do get results in some cases, and in crime investigation hypnotism is slowly gaining acceptance as a means of clarifying a witness’s hazy memory.¹⁴ Hypnotists are able to help in various psychological disorders, and implant posthypnotic suggestions that help people with weight and smoking problems. However, failure or success depends a lot on the skill of the individual hypnotists, and there is no reliable way to predict results, despite the claims of hypnotists who seek to promote themselves.

The operators who run weight loss clinics and anti-smoking clinics are in a similar position. While there is no doubt that reducing excess weight and stopping smoking are beneficial, how to do it best is the controversy. Despite the proliferation of novel ideas, doctors, dieticians, and many layman understand that the

only way to lose weight is to take in fewer calories than are burned. The only method of effective, long-term weight loss is for the person to modify his eating so that he eats consistently just enough to counterbalance his calorie burn. Less, and he'll lose weight. More, and he'll gain weight.

Similarly, the only way to stop smoking is to stop. Very many people have tried to taper off without success, and others who try to stop but backslide by mooching an occasional cigarette soon provoke the comment, "You haven't stopped smoking, you've just stopped buying."

Such clinics vary in effectiveness. Obviously, not everyone will succeed, as motivation is very important. The key to whether these clinics are frauds or not is in the motivation of the operator, and this is very hard to ascertain. We can't judge totally by results for, as we have seen, intense efforts by sincere and well-motivated people can fail, as in the case of the artificial heart.

"Counselors" are special cases. The term is often a simple device to practice clinical psychology while avoiding prosecution. Many states require that anyone who practices as a psychologist be licensed, and to obtain a license the applicant must have passed a certain course of study, and fulfilled other requirements such as practical experience under the supervision of a licensed psychologist.

Mental healing, if we can call it that, is not a science. Unlike the physical sciences, there are no tangible objects to measure, and there is often disagreement as to what doctrine or treatment is correct. Physicians who embark on mental healing are called psychiatrists, unlike psychologists who have extensive psychological training but no medical degree.

Those who don't have training in one field or another, or insufficient training to call themselves doctors or psychologists can, in many states, call themselves "counselors."

Counselors come in many shapes, sizes, and degrees of competence. Some may be actual psychologists, complete with Ph.D.s. Others are graduates of obscure colleges, or even diploma mills. In some areas, they have no qualifications at all.

Treatment of mental problems is at best uncertain. The “legitimate” psychiatrists and psychologists disagree about the structure of the mind, the extent to which physical factors affect the mind, and ways to change behavior and suppress symptoms of mental disorder and to help the patient adjust to his situation. The psychiatrist looks down upon the psychologists, and the psychologists themselves follow different “schools” of thought. Certain charismatic and well-known practitioners have established “schools,” or followings, which adhere to their theories and usually are named after them, such as Freud, Jung, Horney, Sullivan and White. The various “complexes” which they blame for mental problems have often turned out to be normal emotional development or even nonexistent except in the analyst’s mind. In conventional psychiatry, the emphasis has been on treating mental problems with physical methods, such as shock treatment, psychosurgery, and drugs, most of which have proven to have side effects which are more severe than the disorder.

Often, treatment of an emotional problem, from psychosis to relatively modest marital problems, has consisted mainly of “psychotherapy,” in which the practitioner attempts to establish rapport, or confidence, with the patient, and persuade him to change his way of thinking and his behavior. This process bears a remarkable resemblance to both salesmanship and to religious experience, in which the main ingredient is faith.

Taking up the question of how much harm is done by “counselors” who don’t have “legitimate” credentials, we must consider that many people with emotional problems derive no benefit from “legitimate” practitioners. Emotional problems, being intangible, are more difficult to diagnose and treat. There is no tumor to cut out, no fever to bring down.

Some psychosomatic illnesses can lead a patient to unnecessary treatment and even harm at the hands of a “real” doctor, if he doesn’t recognize the cause. Psychosomatic symptoms, although mainly in the patient’s mind, are no less real than physical ones and often doctors apply physical measures to cure them. One category, called “polysurgery” leads the patient to consult surgeons in attempts to have surgery performed.¹⁵ In such

instances, conventional and reputable surgeons perform multiple unneeded operations upon these patients, with the usual risks of side effects that apply to all surgery.

In conventional medical practice, a new word has sprung up. "Iatrogenic" means **symptoms** and disorders caused by the doctor's treatment. A drug side-effect is iatrogenic. Complications of surgery are iatrogenic, all of which confuse the picture further.

The patient with a psychosomatic disorder, who consults a quack who is not permitted or likely to attempt surgery, at least saves himself the risk of complications. The one with an imaginary illness who consults a faith healer may even be "cured" of his disorder, without risky medical treatment.

This brings us to the question of faith and religious healers. Most of us have seen various religious figures who claim to heal the sick, and some of us have seen those who do this on television. There is cause to believe many of the symptoms are psychogenic. However, the imaginary paralysis or pain is no less real than one with a physical cause, as we've seen, and a psychological "cure" can be just as real as a physical one.

Religious healers comprise a gray area in our society and in our law. It is almost impossible to prosecute them, as they enjoy the protection of the First Amendment of our Constitution. In instances where money changes hands, or the practitioner operates a well-known fraud, prosecution is possible.¹⁶ There are well-known bunco schemes based upon fraudulent religious practice. However, many religious practitioners are sincere, and whether their healing is valid is often hard to either establish or disprove.

Another area protected by the First Amendment is health care books. Each year brings its crop of diet books, and volumes on foot reflexology, iridology, and other forms of alternate health care. Each year those who have bought one or the other diet book and failed to lose weight buy a new one, hoping that the latest "system" will help them lose weight.

This is a lucrative field, because of the freedom to publish anything without either censorship or the obligation to check the material for validity. Thus, anyone can write anything he wants,

without fear of accusations of charlatanism. It is perfectly legal, and often the only concession to the law is a disclaimer to the effect that the book is not intended as medical advice, but for informational purposes only.

Another very lucrative field is health food. The very real, and widely publicized, instances of large food producing companies using additives which are carcinogenic or which have other harmful effects has been a windfall for small hucksters who have touted their products as “natural.” A pound of unrefined sugar, for example, sells for many times the price of the refined product, despite the less complicated processing. Sea salt commands a higher price, bought by people who believe that in using it they will get more essential elements than they do from refined salt (true), but ignoring the fact that our oceans are now polluted and they’ll get their share of that, too.

All told, the field of health care can bring wealth to those adept in exploiting it. Unscrupulous frauds are not confined to the fly-by-nighters, but are used by even the “legitimate” practitioners, which makes it that much harder for the consumer to protect himself.

NOTES

1. *Classic Mail Frauds*, Scot Tinker, Eden Press, 1977, p. 32.
2. Personal knowledge of author. At the time, the author, who interviewed this “Doctor of Psychology” for a newspaper, visited his home and became well-acquainted with him. Although some of the statements this bogus psychologist made did not ring true, at the time the author accepted him as genuine because the state department of corrections had.
3. Personal knowledge of author, who works in the printing trades. Anyone can have business cards, letterheads, and other materials printed without question, and can later use them to convince a victim that he is the head of a corporation, a doctor, etc. While this may seem irregular, it’s important to note that printers are not legally or morally obligated to check out the

provenance of each customer and each job they accept, and that most of them are legitimate, in the end.

4. Personal acquaintance of author.

5. United Press, March 7, 1984. National Semiconductor had failed to perform the required "burn-in" tests on chips sold to the Defense Department, tests which would eliminate defective chips. The criminal indictment resulted in almost two million dollars' worth of penalties.

6. *Fraud Investigation*, Glick and Newsom, 1974, Charles C. Thomas, Publisher, pp. 234-5.

7. Personal experiences of author, who has been kept waiting in doctor's waiting rooms for appointments. In one instance, the doctor was over an hour late, and upon arrival laughingly said to the author, "Well, you don't have anything else to do today, anyway."

8. *Fraud Investigation*, p. 252.

9. Ibid, p. 252.

10. Ibid, p. 252.

11. Personal knowledge of author. An acquaintance, a 23-year old man with testicular cancer, went to Mexico to obtain Laetrile treatments. Some months afterwards, he died of cancer, which had spread through his body.

12. The author's father, who died of lung cancer, was first diagnosed as having pleurisy, and told to take a rest cure at a resort town. Two years later, another M.D. diagnosed his illness as cancer, too late to save his life. The original physician collected his bill nevertheless.

13. *A Compendium of Bunk or How to Spot a Con Artist*, Carey and Sherman, Charles C. Thomas, 1976, p. 197.

14. *Law and Order*, periodical, February 1984, pp. 52-4.

15. *Man Against Himself*, Karl Meninger, M.D., Harcourt, Brace and Co., New York, 1938. pp. 259-277. The phenomenon of patients visiting doctors and presenting imaginary illnesses is well-known in the medical profession, and these people are windfalls for "knife-happy" surgeons. Medical publications devote very little

space to the question of how many such people are victimized by unscrupulous doctors. It's easier to ignore the problem, or to pretend it does not exist. In any case, "whistle-blowers" are ostracized by doctors, as they are in other fields.

16. *Fraud Investigation*, pp. 253-255.

SPECIAL NOTE ON SOURCES:

In all the literature examined to gather background material for this chapter, there was no mention of the *placebo effect*, which often operates in obtaining "cures." The placebo effect is well-known to doctors, and even more to researchers. A patient will sometimes get well even through the administration of an inert substance. For some, a sugar pill or an injection of sterile water will cause remission of their symptoms.

Medical researchers use this in checking out new drugs. A group of patients used for the test is divided in two, with one half getting the new drug and the other half the placebo. Neither group knows whether the "drug" it gets is the placebo or the real thing. It often happens that the group getting the placebo has a certain number of successes, and the measure of the new drug's effectiveness is the difference in success rates between the group getting the actual drug and that of the control group, which gets the placebo.

There are several possible reasons for the placebo effect:

1. The body heals itself in many instances. A headache will eventually disappear, pill or no pill.

2. Suggestion is a very powerful mechanism. The healer, by telling the patient that his treatment will help him, uses suggestion. This works better with some people than with others.

3. Faith and other psychological factors. We could say that "faith" is another term for "suggestion," but there are some as yet unexplored and unproven psychological effects involved in cures. These intangible factors explain partly why a certain patient will fare better with one doctor than with another, or with an alternative practitioner better than with a conventional M.D. It is not always fraud, but the psychological mechanisms in both are very similar.

INCOME OPPORTUNITY AND JOB OFFER FRAUDS

Each day, there are advertisements that begin with "Make Money at Home." Generally, these are ripoffs, but they come in so many varieties they're worth a close look.

The simplest type is the "training school" ad. There are legitimate training schools, and most of these offer classroom instruction in technical subjects such as electronics and air conditioning repair, their only fault being that they tend to exaggerate the demand for these skills in the job market and quote somewhat high rates of pay for those with the skills they teach. This is a good example of where legitimate business overlaps fraud.

Correspondence schools are another matter. Some are accredited institutions, and even have various seals of approval, such as those given out by the Veteran's Administration. Others are sleazy operations that offer the student only the opportunity to give away his money. Among the worst are those that have courses in "detective" training. Whoever sends away for the "free information" gets a brochure that promises him substantial income in a lucrative and growing field. Sometimes, he is further enticed by the promise of "free" equipment supplied with the course. Among the "free" items offered by some are small personal computers and "detective" badges. In reality, the student pays for everything, although there may not be itemization of each item.

Many of these courses offer time payments, sometimes carrying the contract themselves, sometimes passing on the contract to a finance company for a commission.

For anyone considering a correspondence course, it's a smart move to contact potential employers in the field and ask whether they would hire someone who is a graduate of that course, and what the pay would be.

Some advertisements are worded so vaguely that it is very unclear just what the money-making scheme is. Typically, these are full-page ads, filled with blurbs calculated to build anticipation

and induce the reader to send in his ten or twenty dollars without knowing exactly how he'll become rich. Often, these ads will carry a photograph of the operator standing next to a Cadillac, Jaguar, or Rolls-Royce which he claims to own, and promise that those who answer the ad will soon enjoy the same high economic status.

Some earn-money-at-home schemes involve buying a kit of tools and materials, or a machine, to produce goods that the company will allegedly buy back. The cost to the victim can run from a few dollars to many hundreds, and he has to sign an agreement to buy all of his material from the company.

The problem arises when the victim has finished his first lot and sends it to the buyer. Invariably, the buyer returns it, claiming the workmanship is not up to the company's quality standards.¹

A variant of this tactic is to offer materials to make a product which the company claims the victim will have no difficulty in selling to his friends and neighbors or door-to-door. The product is not as easy to sell as the company claims.

Employment agencies offer great opportunities for fraud of one sort or another. Although almost every locale in the country has a branch of the state employment service, and almost every newspaper carries legitimate employment ads, there are still "private" employment agencies that offer jobs to applicants. Some of these agencies are legitimate, but others are not.

Theoretically, an employment agency works for the jobseeker, because it collects the fee from him. Most often, the applicant is required to sign a contract in which he agrees to pay a percentage of his first year's salary, or one month's wages, for the job referral. Sometimes, it's hard to see what he gets for this.

One marginal operation, operating in a state in which there was a constant supply of newcomers, earned fees by simply referring the applicant to the telephone company's employment office, after a cursory interview. The operator did not even disturb himself by trying to match the applicant to the job. Most referrals did not find employment at the phone company, but those who did were legally required to pay the agency a substantial fee.

In theory, the agency operator contacts employers in an effort to find a job to suit the applicant. As we've seen, some operators don't work very hard at this. Others have schemes in which they're in collusion with some local employers with flexible ethics. They give the employer a kickback taken from the fee that the applicant pays them.

Sometimes, the side-effects of this practice can be very pernicious. The foreman or manager of a company that uses mainly unskilled labor, for example, knows that he'll get a kickback for each person whom he hires from a particular agency. This gives him an incentive to fire or lay off employees and hire new ones, of course accepting referrals from the agency which pays kickbacks. This practice does not work well with skilled labor, as employee turnover causes problems in that new employees need a period of "breaking in" to their complex jobs.

In major cities, there are resume writing services that offer a reasonably professional product for the fee. However, even this "service" is open to exploitation by the con artist. The scheme is very much the same as the bogus employment agency, so we'll look at them in parallel.

The operator rents an office and places his advertisements offering jobs. He tells the applicants that he'll refer them, or send out their resumes, explaining that he will not collect a fee until the applicant is in his new job.

After a few days, the operator notifies the applicant that he has an appointment with the personnel manager of a large corporation that will be opening up a facility in his city. The personnel manager will be conducting interviews in his hotel room, and the applicant has a specific appointment. The applicant arrives at the appointed time for the interview. The "personnel manager" is a confederate who sizes him up for the final stage of the scheme.

He invites those who seem gullible enough for a final interview in a couple of weeks' time. This gives the operators time enough to line up more victims. When the applicant shows up for the final interview, the "personnel manager" tells him that he thinks that he's very suitable for the job, but that he'll hire him in spite of his

having been referred by the resume writing service or employment agency. He adds that the company has had some negative experience with employees not paying their fees and having their wages garnished. He states that those who did had been summarily fired, as the company did not want to be annoyed by acting as a collection agency for a third party. The applicant would have to pay off his fee and present a receipt the next day to enable the "personnel manager" to go through with the final stage of hiring him.

At this point, the applicants who can scrape up the money pay the fee to the operator. After collecting the fees, the swindlers leave town.²

Pyramid sales are another common scam. While there are legitimate dealerships, such as those run by Avon and Fuller Brush, there are those run by fast operators who are only selling dreams to the unwary.

Generally, the scheme is for each applicant to buy a certain volume of the company's products, and set himself up as a "distributor." The fraud artist tells him the products are easy to sell, and the applicant can increase his profits by recruiting "dealers," each dealer buying a certain amount of inventory.

There is usually a lot of hype involved in these schemes. Typically, the operator holds meetings attended by many candidates for dealerships and distributorships. There are films portraying the opulent lifestyles enjoyed by those who have allegedly succeeded in this plan, and enthusiastic statements by shills who claim that they were poverty-stricken until they joined the plan and brought themselves into riches.³

These are called "pyramid" schemes because the success of each level of dealers and distributors depends on winning new victims and selling inventory to them. Very little filters out to the general public, and the products involved are cosmetics, motor products, and other non-perishable goods. The plan, if diagrammed, would look exactly like that of a chain letter.⁴

Another type of fraud that promises its victims substantial income is the invention development scheme. The operator places

advertisements that begin with the word INVENTORS, and goes on to state that the operator's firm specializes in evaluating and promoting new inventions, and assisting the inventor in getting it patented. There are some people who think they've devised a new invention, and if they reply to one of these ads, they'll find the company will tell them their idea has unusual merit, and because of this, the normal fee would be reduced. They find out that they have to pay several hundred dollars for processing the paperwork, and sometimes find the company asks them for more money to cover the expenses incurred while promoting the idea to manufacturers. There may or may not be an application for a patent. Most people are not aware that there is no requirement by the U.S. Patent Office that the invention actually work, and there are many thousands of ideas patented that have no value whatsoever.

Whatever the details of the scheme, the basic mechanism is to ask the inventor for more payment from time to time, allegedly to use in promotion of his invention. Although there have been some convictions in this scheme, we still see this swindle advertised today.⁵

There are a lot of people in this country who fancy themselves to be writers, and there is a segment of business that thrives upon these people and their dreams of glory. All of them employ deception to some extent.

While there are legitimate literary agents, and some of the best-known writers work through agents because agents know the market for their writings and can negotiate the best contracts for them, there are also many unknown writers who fall victim to either bogus literary agents or to legitimate agencies whose owners take the opportunity to pick up some extra money on the side.

The operators advertise for writers to send them their manuscripts. Typically, there is a reading fee of from fifty to one hundred dollars. In return for this fee, the agents deliver an evaluation of the work, and if it's good enough to sell, will try to do so.

The dishonest operators will not give honest evaluations, as that would involve telling some of their clients they had no talent and

would be better off spending their time doing something else. Each manuscript, whatever the quality, as long as it is accompanied by the required fee, gets the same answer. The writer “shows promise” but the manuscript is “a little rough” and should be revised and resubmitted, accompanied by another fee, for re-evaluation. If the writer cares to submit other manuscripts, the operator will be happy to evaluate them, too, for a fee.

Sometimes the operator can milk an aspiring writer for these modest sums for an almost unbelievable time. Each manuscript that comes to him is an opportunity to generate repeat business, if he can persuade the writer it’s worthwhile to revise it and resubmit it.

Closely allied to these bogus literary schemes are the subsidy publishers, sometimes derisively called “the vanity press.” They play on the well-known fact that some people will pay substantial sums to see their names in print, and be able to claim they are published authors.

Some of the subsidy publishers are quite upfront about explaining the arrangement, that the author pays the costs of editing, typesetting, paste-up and printing, and the publisher and the author will split the proceeds of the sales in an agreed percentage. Others are not so forthright. They con the authors, complimenting them lavishly on the quality and significance of their work, and suggesting it’s likely to be a runaway bestseller. First, however, there are certain formalities, certain expenses....

Among the correspondence courses advertised are artist’s and writer’s schools. As with other such enterprises, some are legitimate, and some aren’t. Whatever the case, the format is the same. The applicant responds to an advertisement for a “free” aptitude test, which the staff of the school will evaluate. Theoretically, if he shows promise, he’ll receive encouragement to sign up for the school’s course. In practice, the evaluation the victim gets back tells him he shows great promise, and is sure to be a success if he takes the course and polishes his skill, under the watchful eyes of the school’s skilled instructors.⁶ The course runs for many months, is expensive, and the victim can pay as he goes.

Some of the schools carry their own contracts, and allow the student to pay for each lesson as he gets it. The ones run by the most flagrant of the fly-by-nights have the victim sign a credit contract with a finance company, collect the money, and leave town suddenly.

One of the more recent frauds involves employment ads seeking "karate instructors." When the victim applies for the job, he hears, quite logically, that he must be qualified in order to be able to teach. The operator tells him that he needs more training, obtainable at his school, before he can qualify for the job. If the victim bites, he signs up for a course without any guarantee that at the end he'll be "qualified" for the job. This is a device used by operators of store-front self-defense schools to stimulate business, and is a good example of how legitimate businesses can overlap into fraudulent practices.

NOTES

1. *Fraud Investigation*, Glick and Newsom, Charles C. Thomas, 1974, pp. 220-222.
2. *Short Cons*, Scot Tinker, Eden Press, 1977, p. 32.
3. Personal knowledge of author, who attended one of these meetings while reporting for a newspaper. The atmosphere was contrived, with much shouting by shills planted in the audience, and outlandish promises of how the "dealers" could, with minimal investments, go from rags to riches in an astonishingly short time. The operator later went to prison.
4. *Big Time Operator's Manual*, Scot Tinker, 1977, Eden Press, pp. 42-43.
5. *Classic Mail Frauds*, Scot Tinker, Eden Press, 1977, p. 23.
6. Personal experience of author, who can't draw a straight line without a ruler. He sent in an "artist's aptitude test" completed in the most incompetent way possible, and got back a glowing letter telling him that he "showed great promise," that his latent skill and esthetic perceptions needed to be "developed," and that the school offered a course that would do this, at a one-time-only price that was a substantial discount from the regular price.

INSURANCE

During the Great Depression, insurance companies were the only class of American business that made money consistently. Not only did they survive, but they thrived. Today, insurance companies own many other companies, as they have invested the billions they've collected in premiums, while paying out very little to beneficiaries.

Insurance is a good example of a type of business (auto dealerships and medicine are two others) that started out for a worthwhile purpose and gradually evolved into what amounts to legalized fraud. The basis for the fraud is misrepresentation of the contract and its benefits to the client. Typically, the sales pitch will tell how the plan will give the insured financial protection so he may feel secure. Some pitches, especially the commercials on TV, feature a celebrity who exclaims to the listeners that "you cannot be turned down or cancelled," and the premiums are low and affordable. The reality is quite different, as the buyer will find out when he reads the fine print.

A long-standing joke about insurance is that the company will pay off only if the insured is involved in an airplane crash which takes place at midnight in a subway tunnel on the 29th of February, leap year. The fine print contains so many exceptions and exclusions that often the client does not get the benefits he thinks he will be getting.¹

There is a saying: "read the fine print," which applies to any contract, but especially insurance contracts. This bears directly on the main point: insurance contracts have a lot of fine print, and the reason for this is to make it difficult for the client to understand what he's getting and more importantly, what he's *not* getting. It's wrong to think insurance companies have their contracts in fine print to save on the cost of paper and printing. With their billions of dollars in assets, insurance companies need not worry about that. The real reason is to make the contracts hard to read, especially for elderly people with failing eyesight. The wording of the contract is another story.

Typically, insurance contracts proliferate multisyllabic terminology, including many redundant technicalities in a maze of repetitious dependent clauses, and these polysyllabic redundancies impede, rather than facilitate, comprehension for the person who lacks the requisite training and familiarity. Like this paragraph, they are hard to read.

This is not a coincidence. Insurance companies design them to be hard to read, to make it almost impossible for the client to understand what he is getting and what he's been led to believe he's getting are not the same. Only a lawyer can understand them. Even the insurance salesman often doesn't. He's been instructed in how to pitch the policy to the customer, and how to answer questions. He doesn't have to worry about the fine print, because the sales department does not process claims. When the client makes a claim, he'll find the claims department is far less friendly than the salesman.

NOTES

1. *A Compendium of Bunk*. Carey and Sherman, Charles C. Thomas, 1976, pp. 134-135.

INTENTIONAL ACCIDENTS

Homeowners and small businessmen may often worry about bad checks, but there are more dramatic swindles to which they are vulnerable. One of them is the intentional accident artist, or “flop” artist. There are innumerable instances of “bone breakers” who “accidentally” throw themselves in front of automobiles and collect for their injuries. One unpleasant fact which confuses the issue is that some injuries, while real, are intangible, as in whiplash of the neck. It is a well-documented fact that whiplash can cause lingering symptoms, such as pain and dizziness, but it’s also true that these symptoms cannot be detected, measured, or verified by any tests. The doctor, the lawyer, and the insurance company have only the sufferer’s word. There are many compliant doctors and lawyers who help to magnify any symptom, legitimate or not, that the victim suffers in order to extract as large a settlement as possible. In one instance, a firm of lawyers advertises on television that one of the partners, besides being a lawyer, also has a medical degree.

Considering outright frauds, we come to the “rusty nail” swindle. The fraud artist orders a meal in a restaurant and while eating, makes a cut inside his mouth with a razor blade. He yells, and spits out a rusty staple or nail. Claiming that the offending item was in the food, he sues, or threatens to sue. As many such suits are settled out of court, the fraud artist often finds it easy and quick to extract money from the scheme.¹

A variant on this personal-injury theme is the “spilled wax” swindle. The con-man, playing the role of customer in a supermarket or other retail outlet, uncaps a bottle of liquid wax while unobserved and spills some on the floor. The substance need not be wax, as there are many items and compounds that can make a floor slippery, such as ice, a banana peel, etc.

When another customer appears in the aisle, the con man “takes a fall,” crashing to the floor and feigning dazedness. Of course, the other customer will usually try to help him, having been a witness to the incident, and the store manager will rush to the scene. The

victim takes a trip to a hospital, complaining of pain in the head and neck. This sets the scene for a lawsuit, the threat of a lawsuit, or a quick settlement out of court.²

A businessman or his insurance carrier, while they may be suspicious, often have no defense against this practice. Insurance companies, as a means of protecting themselves against such scams, keep detailed records of claims against them, in the hope of establishing that the complainant has a record of prior claims, which would count heavily in court if the insurance company can show a pattern. This technique does not always work, as many con artists use false identities in these games.³

NOTES

1. *Professional Con Games, Schemes, and Frauds*, 1979, Carl Dorski, Roadrunner Publications, PO Box 572, Keego Harbor, MI 48033, p. 19.

2. *Ibid.* p. 20.

3. *The Paper Trip, I and II*, Eden Press.

INTERNATIONAL FRAUDS

Crime, like business, does not stop at a nation's border. For both legal and tactical reasons, it often pays for a criminal to operate in two or more countries. An act that calls for a heavy sentence in one country involves a lesser penalty in another. It may not even be illegal. For example, a quirk in the counterfeiting laws of most countries makes it illegal to counterfeit only that particular country's currency, but says nothing about another's.

Other countries make good hosts, perhaps because they permit secret bank accounts, or have no extradition treaties. Switzerland and Brazil are traditional examples of this.

The most practical reason for operating across national lines, especially for the con man, is he can depend on the usual lack of cooperation and coordination between police forces to work in his favor. There are jurisdictional limits. There are language barriers.

Let's look at a real-life example to see how this works:

Paris, France, in 1969 was a good place for an American tourist speaking French. The food was good, and prices had not yet risen out of sight. An American couple getting off a tourist river boat was approached by a young lady:

"Pardon me, but you look like you're from the States."

"Yes we are."

"Well, we're having a little get-together for Americans tonight at the ——— Hotel. We'll have a buffet supper and some films. Would you and your wife like to come?"

That was the approach, delivered by an American girl studying in Paris and picking up some extra money by greeting marks and "steering" them to the main operation. Possibly she had no knowledge of anything beyond her very limited part in the scam.

When the couple showed up at the hotel, they found a dining room set up with a buffet table at one end. They gathered their meal together, sat down, and soon the salesman assigned to their table joined them. During and after the meal, the hosts showed films of a "vacationland paradise" in Florida, and the chief

salesman explained that the assembled guests were getting a once-in-a-lifetime opportunity to invest and get rich.

In front of each place at the table was a small stack of papers. On top was a brochure, in color, telling of the land offer. At the bottom of the stack was a legal document issued by the Florida Land Commission, with some warnings on the top page. The warnings stated clearly that it was advisable to inspect personally any land offered, as it might be under water or deep in a swamp. When the husband lifted the other papers by a corner to peek at this bottom document, the salesman firmly slammed his palm down on the stack.

The rest of the evening was a typical "high-pressure" sales effort. One couple bought a parcel of land, early on, and the master of ceremonies loudly announced that "Parcel 101" was going out of circulation, and no longer available for sale. He had the buyers stand up and take a bow, and announce their reasons for buying. The M.C. visited each table, to oversee the proceedings. As the session drew on, the crowd began to thin out, most of the people not following the example set by the shills early on.

Among the last to leave were the couple we've been following. Fascinated by the affair, they stayed to hear it all, carefully refraining from signing anything. They earned the M.C.'s personal attention, and perhaps personal wrath, when he stopped at their table to inquire why they hadn't bought this tremendous offer. He turned offensive when he stated: "There are only two reasons why you haven't bought. Either you don't have the money or you don't trust me."

Instead of embarrassing the couple into signing, this challenge offered them a quick out. They simply pleaded poverty, telling the M.C. they'd saved for five years to come to Europe and only had their tickets and a few traveler's checks to their name. It was an outrageous lie, but no worse than the lies they'd been hearing all evening. They got up and left.¹

Now let's examine closely what might have happened if they had signed, paid a deposit, and found they had been conned.

1. To whom would they have complained? The Paris Police? That depends on when they found out they'd been taken. The

property was in Florida, and neither husband nor wife had ever been to Florida. If they happened to go, and found their “recreational property” under water, and complained to the local sheriff, they’d surely be told the fraud was not committed in Florida, and they should complain to the police where it was.

2. Traveling around to investigate and make a complaint would be costly. Who could afford it? Who’d be able to take the time off from work?

3. Who can or will prosecute? Prosecution, difficult as it is, does happen when a fraud takes place in a local area, but an international affair such as this one creates a nightmare. A fraud, perpetrated by Americans only on other Americans who will not be long enough in Paris either to complain to the police or to testify if a prosecution should result, is an almost perfect bunco operation. It is patently illegal, but under whose law? The difficulties of following through with a prosecution are almost insurmountable.

NOTES

1. Personal experience of the author.

MONEY SWINDLES

There are several swindles that involve cash directly, and which fraud artists use on both ordinary citizens and small businessmen. Some are crude and simple, and others are so ingenious it is almost impossible to provide an adequate defense.

One of the oldest ones is check kiting. This term refers to establishing a checking account with a small balance, then drawing a check to establish another in another bank. The amount is larger than the funds in the first account, and the con man covers that check with one drawn on the second account. He then covers the one in the second account with an even larger one which he draws on the first account.¹

This is the plan for simple check kiting, but there are more elaborate schemes, involving many accounts and a system of rotation to cover all of the bogus checks. In the complicated systems, it's critical to keep detailed records, and timing is extremely important to keep the different checks floating between the banks without running into each other.

One question that inevitably comes up when a class in elementary economics discusses kiting is: "Why is check kiting illegal, if all the checks are covered?" The reason is that, although the game may go on for months, the last check will not be covered. The amounts in the accounts may be fabulous, but they exist only on paper, and there is no "real" money to cover them.

Kiting is an old fraud, and does not work well anymore, for several reasons:

1. Today, it's common practice for banks to delay crediting an account with the amount of a deposit involving a check until the check clears. This is not a perfect defense, as with the elaborate systems a check can clear and be credited, but it stops the simple systems.

2. Bank employees all know what kiting is, and they're alert to the possibility of a checking account's being established for kiting. Kiting checks presents a pattern of deposits and withdrawal by check, with a deposit being followed by a check drawn for a larger

amount, followed by a deposit for an even larger amount, etc. The computers that post checks and deposits to the individual accounts are programmed to “flag” accounts that show a pattern that suggests kiting.

3. Electronic banking cuts the time needed for a check to clear drastically, and it is no longer possible for a check to float between accounts for weeks. The decline in the speed and efficiency of the U.S. Postal Service also works against check kitters if they bank by mail.

The phoney loan agency is another money swindle. A person who applies for a loan meets a sympathetic gentleman who assures him his *bona fides* appear good, and there should be no problem in securing the loan. However, the formalities include a background check, involving some expenses, and the prospective borrower must put up the front money for this. If the victim bites and passes over the money, he'll have a wait of several days or weeks before he gets a sympathetic letter informing him that, on the basis of the information developed in the background check, the request for the loan must be denied.²

There are several variations possible on this theme. This swindle is an easy one to work by mail, as all of the transactions can take place on paper, instead of with a face-to-face meeting. As the amounts involved can't be very large, the swindler must be able to continue operations in order to make substantial amounts from this scheme, and the critical part of the swindle is the “block,” the device to keep the victim quiet while the swindler carries on.

The “block” is the loan application, which contains the statement that the fee required for background investigation is not refundable. Unless the victim is very perceptive, or very suspicious, he will not complain to the police, thinking that this legal document is legitimate.

Bad checks plague businessmen, and most retailers have established procedures by which the customer who offers a check must prove his identity, or present a check guarantee card that is valid only up to a certain amount. In cases of large checks, the businessman will check with the bank by telephone to verify there

is enough deposited in the account to cover the check. The clever swindler has an almost fool-proof way around this precaution. He opens a checking account at the bank, issues a few checks, then returns to the bank to report that he lost his checkbook or had it stolen, and requests that the bank close the account and start a new one. He makes a substantial deposit into the new account, enough to cover the amount of any purchase he plans with his scheme. When he gets the printed checks, they'll have his name, address, and phone number on them, with only the magnetically imprinted account number being different. However, the first digits of the two account numbers, identifying the bank and branch office, will match, as they'll have come from the same branch.

Working the swindle, the fraud artist makes an expensive purchase at a store during banking hours, the amount involved being so large that the store employee feels compelled to verify the validity of the check with the bank. The check which the con man hands over is drawn on the legitimate account. The telephone check establishes the validity of the account, and when the clerk returns with the check the con man decides on a different purchase and tears up the check, writing a new one from the check book belonging to the closed account. If he is especially nifty, he may write a check for more than the amount of the purchase, asking for the difference in cash, as long as the total does not exceed the amount that the clerk or manager had verified with the bank. Retailers almost never notice this switch.³

Another swindle, somewhat riskier but often pulled on retailers, is the Secret Service Agent Swindle. To carry this out, the swindler obtains a U.S. Secret Service letterhead. This is easy to do, requiring only a letter to the Secret Service on an unrelated matter. On a separate sheet of paper, the swindler types a circular pertaining to a new issue of counterfeit \$100 bills that have come into circulation, and tapes this circular to the legitimate letter which he's received from the Secret Service. He photocopies the letter, placing a hundred dollar bill with the serial number enumerated in the letter at the bottom of the copy, below the signature of the genuine Secret Service Agent who signed.

The con man's partner, using this perfectly legitimate hundred-dollar bill, makes a purchase from a retailer. Later, before the retailer makes a cash deposit at his bank, the "Secret Service" man appears, shows the merchant forged I.D., and informs him that he's tracking down a new run of counterfeit that has appeared in the area, showing him the photocopy of the letter to substantiate this statement. Asking the merchant if he's taken in any hundred-dollar bills, he examines them. When he comes across the one his confederate used earlier, he picks it out and shows the merchant that the serial numbers match. He tells the merchant he must take the bill with him for "evidence."⁴

Another swindle having a revival is the "bank examiner" fraud. The fraud artist, posing as a "bank examiner," FBI agent, or other official, approaches his intended victim and asks him to cooperate in an investigation involving a dishonest teller at his bank. He asks the victim to withdraw a large sum of money from the bank and pass it on to the agent for "evidence," which will help to put the dishonest teller behind bars. The con artist tells the victim the Government will redeposit his money shortly, when the investigation is completed. He may even give the victim a receipt for the amount.⁵

All of these swindles work, and some work very well indeed. Some of them work only on very gullible victims, and others are so fool-proof they'll work on almost anyone. The bank examiner fraud seems to work best on the elderly, as they are the ones most often victimized, possibly because they come from an earlier, simpler era, when people appeared to be more honest.

NOTES

1. *Big Time Operator's Manual*, Scot Tinker, Eden Press, 1977.
2. *Crooks, Con Men, and Cheats*, Eugene Villiod, Gambler's Book Club, 1980, pp. 66-68.
3. *Clipping the Flocks*, Scot Tinker, Eden Press, 1977, p. 25.

4. *Professional Con-Games, Schemes, and Frauds*, Carl Dorski, Roadrunner Publications, 1979, pp. 12-13.
5. *Short Cons*, Scot Tinker, Eden Press, 1977, p. 7.

MOVING GOODS

Along with deceptive advertising, deceptive merchandising has been with us a long time. The line between them is hard to define, as is the line between legitimate business and fraud.

Apart from “gimmicks” used to make the merchandize more attractive, there are financial incentives. We’re so familiar with the phrase “for a limited time only” that often we don’t even listen to it. We’re also very familiar with “sales,” as most stores have a “sale” of one sort or another every week.

While the “sales” offered by legitimate stores are real, in the sense that they are reductions of the established price, we ought to be wary of the reason behind them, and exactly how they work. They are “loss leaders,” items which sell at little or no margin of profit, or even for lower than cost, in order to entice customers into the store. To make up for this, other items are overpriced. Indeed, it may even happen that the item on “sale” is available elsewhere for even less money.

When this happens, there’s cause for suspicion that the item was not really on “sale” at all. False or inflated “list” prices are common gimmicks. In some areas, such as cameras and electronic equipment, “list” prices are unrealistically high, set that way so that the merchant can give the customer a “discount” every time.

Some glittering goods, usually cameras and jewelry found in stores located in tourist areas, come with several price tags apiece, so that the merchant can choose his preferred list price and claim to offer whatever discount he feels will be most effective.

There are also other gimmicks used to give the impression of a “sale.” Wheedling phrases such as “made to sell for” imply that the value of the item is higher than it is, and that the merchant is discounting it. Keeping in mind that a legitimate sale price is one that’s lower than the usual selling price, we find other goods being moved by the claim of “special introductory offer,” which implies that, although the item has just come on the market and there is no base price for comparison, the selling price will go up after the “offer” is over, and of course the offer is “for a limited time only.”

In most large cities there are certain areas that are full of "tourist traps." The Times Square area in New York is one, with each block lined with stores festooned with colorful signs proclaiming "sales." Many of these are "going out of business" sales and some are "going out of business today" sales. Some of these stores have been "going out of business" for several decades.¹

Some of the "sales" are for items which the customer knows sell for much more elsewhere. It often happens that these prices are far below even wholesale, and the suspicion comes up that these must be stolen goods. More likely they are counterfeit or "seconds," defective goods. In many cities, there are stores that specialize in "seconds," lots of merchandise that do not meet the manufacturer's quality standards. Sometimes the defects are severe, but more often, as in clothing, the defects are such that the value and serviceability of the item is not reduced, as when the cut on a panel of clothing does not line up with the pattern of fabric.

Flea markets are excellent places for moving stolen goods as well as defective ones. These merchants, with shops that consist of collapsible tables, present an image like that of a Middle East bazaar. "Let the buyer beware" is certainly in force here. It's sometimes possible to detect defective material, but stolen goods carry another danger to the buyer. A good example is the flea market merchant who sold a top-of-the-line make of typewriter for one hundred dollars. These were not defective, just stolen, but yet a good deal for the buyer who did not question too closely. The problem would arise when the machine needed service or repair, because the manufacturer keeps a computerized file of all stolen machines, and requires the network of repair facilities to report all serial numbers of machines serviced to the central office. Whoever brought in such a machine might face charges of criminal receivership, unless he had a bill of sale to prove his purchase. Bills of sale are not common at flea markets. With luck, the buyer would only have to live with confiscation of the machine. Finding the merchant to recover the purchase price might be a problem.²

The surplus goods game is common, with many variants. Typically, the con artist, driving a truck and dressed appropriately, rings the doorbell. He explains that he had an order to deliver a

load of fertilizer to someone down the street and that the buyer changed his mind. He adds that the load is not worth carting back, and that he's willing to sell it at cost or less to anyone who'll buy it. This story has many versions, and the material involved can be television sets and other appliances.

In moving goods, the "television game," although cumbersome, is one con that does not involve any actual appliances. The con man telephones an office, claiming to be the friend of a friend, and tells the listener that he can offer him television sets or other appliances that a local department store is selling as surplus for a very low price. He may try to hustle the sale by saying that the appliances are available only in small lots, and entice the listener into persuading several fellow employees to join in.

If the victim bites, the con man instructs him to meet him in the parking lot or the lobby of the store with the money. When the patsies show up, the fraud artist takes the money and instructs them to move their vehicles to the loading dock to collect the merchandise. The victims wait forever.³

The dangers of buying large-ticket items sight unseen are highlighted by the case of a furniture store that advertised "sale" items through the electronic media and the mail. This store used false list prices and misstated "sale" price, claimed that some sales were for "one day only" when they were not, substituted floor samples in their shipments, selling them as new, and shipped items different from those ordered.⁴

It pays to be suspicious of unusually good deals that seem too good to be true. They often are.

NOTES

1. Personal observation of author.
2. The stolen typewriter situation was explained to the author by a friend who is in the service business and who also attends flea markets regularly.
3. *Short Cons*, Scot Tinker, Eden Press, 1977. p. 8.
4. *Classic Mail Frauds*, Scot Tinker, Eden Press, 1977, p. 22.

PERSONAL DECEPTIONS

This section will start with a lighthearted deception before moving on to more serious ones. Occasionally, a man seeking to seduce a woman will, if he has the nerve, take her into a jewelry store on a Friday afternoon, immediately after the banks have closed. Buying a very expensive watch or piece of jewelry for her, he'll pay with a check. The salesman will point out to the couple that the store cannot release the merchandise, on a purchase of this size, until the check clears, and the soonest that can happen will be Monday. The couple, accepting this with good grace, leaves.

Monday, when the store employee calls the man to tell him there are not sufficient funds in his account to cover the check, the man replies; "I know, but thanks for the wonderful weekend!"¹

The foregoing account sounds like a legend, the sort of story heard at a smoker, rather than a real case history. The following ones definitely *did* happen, and similar incidents continue to happen:

The hitchiker may not be what he seems. While we hear many cautions regarding the picking up of hitchikers, some are very attractive types, and behave properly once in the car. One such told the man who had picked him up that he was out of work, had run through his unemployment insurance, and was traveling on to try and find a job in a new town. The driver was very impressed with the young man's sincerity and clean-cut manner. He continued to question the young man, and found that he'd slept in a bus depot the previous night, and hadn't eaten that day.

They arrived in the driver's home town as night was falling, and the driver suggested that the young man come home with him to have supper, mentioning that his wife was a good cook. The young man appeared reluctant, not wanting to be a bother, and this convinced the driver further of the young man's sincerity and honesty. They proceeded to the driver's house, where the man's wife served them a satisfying supper. The young man seemed so well-mannered that they invited him to spend the night in the spare bedroom.

During the early hours of the morning, the driver woke up to find that the young man was gone, along with his wallet, money, and his car.²

The “business partner” scam can work in several different ways. In one instance, a man approached the victim, claiming he was in the jewelry business, but ill health made him devote less time than he should to running his business, and he was seeking a partner to help in the day-to-day affairs. The victim invited him home for supper, and during the meal the conversation turned to pieces of jewelry owned by the host’s wife. The con man, upon seeing them, told her they were more valuable than she’d thought, and offered to take them to one of his business contacts for a formal appraisal. They turned over the jewelry to him, and he left. Several days later, when the victim wondered why he had not heard from the potential “business partner,” he tried the phone number on the business card the man had left, and found that it was a phoney. The man never returned.³

The publisher of a struggling weekly newspaper hired a man who claimed he had over a million dollars in a Swiss account, which he’d be glad to invest in the newspaper to help it over the current crisis. There was one problem. To get the money out of his account, he had to appear in person in Switzerland, and he could not leave the country because he was on parole from prison. He had been in prison because of a conviction for fraud, a fact that the publisher, who surely thought himself to be a canny businessman, ignored.

The publisher hired him as an advertising salesman, or “Account Executive,” and the con man sold a few ads while he supposedly worked on the problem of getting his funds out of Switzerland. He ran up large balances on the newspaper’s credit cards, made many international phone calls to “business contacts” and “lawyers” in both Europe and Hong Kong, all of them on the newspaper’s lines. He floated around the office, telling anyone who had the time to listen about his impressive business deals and contacts in Europe, showing letterheads and business cards as substantiation of his claims.

The game eventually came to an end, as the publisher gradually realized that all he was going to get from this man was more bills and more excuses regarding the delay in the transfer of funds. By the time the publisher woke up to the fact that the ex-con he'd hired was milking him, he'd lost several thousand dollars.⁴

The "baby burglar" is an almost irresistible con, as most people are very compassionate regarding children. The doorbell rings, and when the householder opens the door there is a woman with a baby, who explains the baby is thirsty, shows an empty baby bottle, and asks for some water. The con woman, who may or may not be operating with a partner, uses the distraction to lift a wallet, purse, or any valuables that are easy to pocket.⁵

There are endless variations on the theme of using an excuse to gain admittance in order to commit a burglary. One woman was victimized by a person claiming to be a religious proselytizer. The victim let the other woman in, as she explained about her church and its doctrine. At one point, discussing the victim's work, they went into the bedroom, where the victim showed the woman a dress she was making. After the proselytizer had left, the victim noticed that her purse was missing.⁶

Once the con artist or burglar is in the home, there are all sorts of distractions and dodges to get the victim out of the room so he may "toss" the room and "lift" whatever is easy to take. If the victim offers a cup of coffee, that gives an opportunity of several minutes' duration. Asking to use the bathroom is an almost foolproof way, as few victims will accompany the con artist through the house to the door of the bathroom, unless the layout of the house is so complicated that the bathroom is truly hard to find.

If the telephone is in another room, an accomplice can phone the victim, getting him or her out of the room for a short while. A request to use the phone, on the other hand, is a door-opener. It's hard to resist someone who claims to have had a car breakdown and who asks to call for help. Sometimes, the phone call can serve as a cover for a theft by stealth, but at other times the crime is violent.

What many people with unlisted numbers don't realize is how easy it is to find out the number, even without the "friend in the phone company" so often cited in the "how-to" books and detective novels. A request to use the phone to cope with an emergency will almost always produce results. The conventional advice to homeowners is never to admit anyone, but to ask for the number they wish to contact and place the call themselves. This will prevent a burglary, but will disclose the unlisted number if the number the con man provides is that of an accomplice, supposedly the owner of a garage. He tells the person calling that it will take a couple of minutes to contact a tow truck on the radio, and asks for the phone number so that he may call back.

NOTES

1. *Clipping the Flocks*, Scot Tinker, 1977, Eden Press, p. 17.
2. *A Compendium of Bunk*, Carey and Sherman, 1976. Charles C. Thomas, pp. 56-58.
3. *Ibid.*, p. 59.
4. Personal acquaintance of the author.
5. *A Compendium of Bunk*, p. 61.
6. *Ibid.*, pp. 61-2.

PERSONAL IMPROVEMENT

There is a whole category of groups and services that fall loosely under "personal improvements." These do not train in job-related skills, but in ways that enhance the way a person feels about him or herself.

The first we'll consider is part of what we might call the "Fear Industry." It's true, the crime rate is at an all-time high, and street crime in America gets a lot of publicity. It's also true that the fear of crime that grips a lot of people gets extensive coverage in the news. Given this, it's no surprise that many store-front "schools" have sprung up to teach various forms of self defense, from karate and other types of hand-to-hand combat to techniques of handling firearms for personal protection. Some of the instructors are competent. Most are not, as the motive is quick profits, not high-quality instruction. This is especially true in firearms instruction, for unlike the karate schools, there is no national association, no system of accreditation, and no set of standards that they must meet to qualify as self-defense schools.

Usually, the trappings and atmosphere are designed to pass the instructor off as a "tough guy" who can handle himself in any situation. Often, the instructor wears camouflage clothing and has a pistol tucked into his belt, as if expecting an imminent attack. He may claim to be a former Green Beret, or policeman, as qualification for teaching firearms defense. He may have gotten all of his shooting experience from competition in "Combat Matches," which differ seriously from conditions on the street. Often, the shooting techniques the instructor teaches are more suited to competition than the street.

As cost is a factor, the courses often are short, giving the student very little. As with any skill, it takes time to develop proficiency, and even the best and most dedicated instructor can do only so much. If the operator of the school is dishonest, he'll promise more than he can deliver, claiming to be able to make the student the equal of any street situation in just a few weeks of part-time instruction.

One school offered a course labelled “ranger training,” designed supposedly for the survivalist or paramilitary type. Unfortunately, the students did not even get the level of “training” of the “weekend warriors,” the National Guard, as they had class only on Sunday afternoon, during which the instructor taught them how to fight the Vietnam War over again. Possibly none of the students realized that it takes much more time than a few Sunday afternoons to turn a young person in good physical shape into a Ranger.

A few years ago, “sensitivity training” was the fad. There were various versions of “sensitivity training” offered by “psychologists” and various “institutes” around the country, all at high prices. These “encounter groups” would hold regular meetings during which the members were encouraged to bare their deepest feelings, the process sometimes aided by a requirement of total nudity.

The alleged “benefits” of this sort of experience were often unclear, with each “institute” and street-corner psychologist peddling his own version. What they all had in common was a high price. Like other types of group affairs, such as smoking and weight loss clinics, their results vary. As in every sort of therapy group, there are certain principles of group dynamics that apply.

There is always a group “leader.” He may be the “therapist,” “guru,” or have some other title, but his job is to direct the group overtly.

There usually is a small number of supporters in the group and these may be called “assistant leaders” or some other titles, or they may not be overt at all, but blending in with members of the group to perform the same functions as “shills.”

It’s a well known fact that most people are conformists to a certain degree. To make people do a certain thing, it’s usually very helpful to show them that others are doing it, too. An example is the disrobing that takes place in some “encounter” groups. When the leader gives the command to disrobe, any who hesitate will see others taking their clothes off quickly, without hesitancy or embarrassment.

A fashionable term for this phenomenon is “peer pressure.” It is the same thing seen in the “brainwashing” practiced in some

countries. The threat of disapproval of the group serves to keep individualistic or deviant individuals in line. It works the same way in groups in this country. The groups offer certain personality changes. The effect comes about by peer pressure and conformism to the attitudes and expectations of the group.

We might legitimately ask, at this point, whether it matters how the effect comes about, as long as it gives the participants what they're seeking. It does matter. Changes produced by the influence of the group can, and often do, reverse themselves after the participant leaves the group. There may be very gratifying effects at the moment, but some months later the ex-member may be asking himself what he got out of it.

It's important to note that these group dynamics apply to all groups, whether they involve mind improvement of a sort, weight reduction, psychotherapy, smoking groups, etc.

Many of these groups depend on the fact that most states do not regulate "counselors," as we've seen in the section on health care. Anyone can put himself into practice as a marriage counselor, psychotherapist, or even "group therapist."¹

Sex therapy has become a fad in recent years. Without a doubt, some of it is legitimate, but some are scams. Some are thin covers for prostitution operations, with clients being given "sex therapy" to "cure" them of a "problem." Perhaps these are the least harmful of the category, as they provide a certain service for a certain price, and that is that.

Others, the ones that claim to "treat" various psychosexual disorders, can do a lot of harm. As with other types of health care, it's difficult to prove that doctors with legitimate medical degrees and licenses do any better, and one of the most obvious facts is that the legitimate practitioners disagree on methods of treatment for psychosexual disorders. However, there is no doubt about the motives of the fraudulent operator.

Some of these operators cater to some of the kinkiest desires, and even gratify them for themselves. Asking couples to have intercourse while the "therapist" watches may be helpful in some cases, but in others it may just satisfy the "therapist's" Peeping-

Tom impulses. Some clients may unwittingly be modeling for pornographic films and tapes, shot by cameras which may or may not be hidden.² Sometimes, there is more than one source of profit for the operator.

Understandably, complaints to the police are far fewer than the number of operators would justify. A man seeking "therapy" for impotence is not likely to be eager to discuss his problem with the police, even if he's been bilked. It may even be that he's already been unsuccessfully treated by an M.D. before he decided to place his trust in a "sex therapist."

NOTES

1. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, pp. 19-20.
2. *Ibid.*, p. 19.

PERSONAL PROPERTY

A way that some con men raise quick cash is to sell the victim a piece of personal property at an attractive price, get payment, or at least an installment, in cash, and then leave town. Some of these schemes may seem simple-minded, but in fact many people fall for them.

One technique is selling a fake diamond by representing it as real. The diamond is usually set into a piece of jewelry, and the fraud artist and the victim go to the jeweler's to have it appraised. The jeweler is often totally innocent and unrelated to the con game. The con man may even encourage the mark to pick a jeweler whom he trusts.

The jeweler appraises the diamond, confirming that it is worth what the con man claims it is. At the first opportunity afterwards, the con man makes the "switch." It is easy for him to do, as he can rightfully retain possession of the jewelry until the mark pays him for it, and it's a simple matter to have a copy of the piece of jewelry in the same pocket as the real one.¹

A variation on this theme is for the hustler to present the mark with a written appraisal showing that the jewelry is worth much more than the asking price, and offering to accompany the victim to a local jeweler to have it appraised once again. The second appraisal is supposedly for the victim's "protection," but it also gives the fraud artist an opportunity to make the "switch." Once he collects the money, he's gone.²

There is a scheme called "block laying" that involves passing off cheap merchandise as very valuable material.³ It is also adaptable to selling stolen merchandise. The tactic is to make a purchase, leaving the piece of personal property as security. The con man can tell a service station attendant that he lost his wallet, needs some gas and perhaps a new battery to get where he's going, and offers to leave his watch as security for the amount he buys. He can dress up his story by claiming to be a member of a musical group and promising the attendant free tickets to the performance, etc.

A nervy, but effective way to raise quick cash is for the fraud artist to sell a rented car. The simplest way for the swindler to do this is to rent a car using a forged credit card, the same one he uses to pay for his hotel or motel room. He then advertises the car for sale at a very attractive price. He can save time, if he does this regularly, by phoning in the ad before he has the car or even before he arrives in town, as usually he can reserve a car and knows which model and make it will be.

When the calls come in, he arranges to meet a prospect in a parking lot near his home. The story he tells him is the crux of the fraud, and the swindler must deliver it in a convincing manner. He tells his mark that there has just been a death in the family, that he's willing to sell the car at a low price to raise quickly the money to fly back home, and that a small deposit, say five hundred dollars, will enable him to turn the car over to the mark. He promises to have his lawyer send the necessary papers for a formal bill of sale and transfer of title, and asks the victim to drive him to the airport.⁴

There is a variant on this method, which enables the con artist to profit several times from selling the same car. This also works with a rental car. The basic idea is have forged papers for the car, sell it to the mark, and then steal it back, reselling it the next day.⁵ There are some items of window dressing that can go along with the basic technique.

One way is for the fraud artist to be a female. To anyone who answers the ad, she can claim that her husband has just left her, thrown her out, etc., and that she's selling the car to get some ready cash. She can also assume the role of having just lost her job, being unable to afford the rent, and needing cash to be allowed to remain in her apartment.

Stealing the car back is the easiest part. In order to sell the car to so many people, the swindler needs some sets of duplicate keys, and he or she uses one set to repossess the car each night.

If the swindler is using forged papers, he can even use his own car for the sale, as he's going to take it back at the end, anyway. It requires some fine judgement, though, to know when to stop

running this scam in one location, as the repetition of stolen auto complaints to the police, all involving the same make and model of car, will sooner or later attract attention.

NOTES

1. *A Compendium of Bunk*, Carey and Sherman, 1976, Charles C. Thomas, p. 141.
2. *Professional Con Games, Schemes, and Frauds*, Carl Dorski, 1979, Roadrunner Publications, p. 7.
3. *Short Cons*, Scot Tinker, Eden Press, 1977, p. 26.
4. *Ibid.*, p. 25.
5. *Ibid.*, p. 37.

PLAYING ON HOPES

There are scams that play on people's hopes, and they cross the lines between categories. Some of them are postal frauds, and others perhaps belong in the "income" category. They all use the same basic mechanism. An advertisement appeals to the person who thinks he has talent, and promises help in developing that talent, and make contacts in the field so that the "talented" person may find employment using that talent.

One fraud started out as a "contest" for lyric writers. Each person who sent an entry received a letter telling him or her that he or she had won, and definitely had talent. Along with the encouraging letter comes a contract, the "prize," which for a fee promises the talent agency will have a music writer compose a tune for the lyrics, a performer will sing the song, and the result will be presented to the decision-makers of various famous recording companies.¹

"Talent agencies" also victimize singers. One amateur answered an ad placed by such a "talent agency" and found that if he handed over several hundred dollars for "expenses" he could perform accompanied by several musicians and have his performance recorded on tape. The tape would then go to the head of a recording company, and he'd be on his way to stardom.² The operator of this "talent agency" collected as much money as he could from aspiring singers, then moved out of his opulent office, sending back the rented furniture.

"Model agencies" are another scam. There are legitimate ones, but there are also the operators who prey on aspiring models. These scams also start off with an ad, sometimes for a "talent contest," and sometimes with a promise to develop the person's "talent." They always ask for a fee, for "expenses." While a reputable agency will, for example, suggest the aspiring model should have a portfolio, the client is free to choose his or her photographer and have the work done elsewhere. The fraud artist will tell the client that the agency has its own photographer and printer, and even offer a "discount." The hit-and-run con man will

collect the money and skip out, leaving the clients high and dry. Others will lead the clients along for quite a time, making a profit from the photography and printing, then suggesting the client needs “coaching” to develop the talent. Of course, the agency will be glad to supply the coaching for a price. The fraudulent part is that the agency makes no effort to contact potential users of that talent, as promised. Some operators are quite skilled at stringing their clients along, telling them they are not quite ready for presentation, and some additional “coaching” will move them another step towards their goal.³

The important point to note, for anyone with talent, is that reputable and honest agents do not charge fees. They work on commission, collecting a percentage of whatever the performer earns. The same is true of publishers and literary agents. Legitimate publishers pay royalties or buy the work outright, and never charge the author for “editing” and other “expenses.” Any agency that demands money “up front” from an aspirant is likely to be a fraud.

NOTES

1. *A Compendium of Bunk*, Carey and Sherman, Charles C. Thomas, 1976, pp. 168-170.
2. *Ibid.*, pp. 163-168.
3. *Ibid.*, pp. 170.

POSTAL FRAUDS

Fraud using the mails has become almost an institution in this and other countries. It is not confined to buying goods sight unseen and later finding out they are defective, but to many schemes of such subtlety and complexity that it's impossible to cover them all in one book.

Unlike the telephone company, the Postal Service is an arm of the government and maintains a staff of Postal Inspectors to police the use and misuse of the mails.¹

Deceptive advertisements are perhaps the simplest form of mail fraud. Some operators cheat the client by not sending the merchandise, and by the time the complaints pour in and the Postal Inspectors come around, they've left town.

Such an operator will probably use a "mail drop," a fake address, not a post office box. Renters of post office boxes must list their correct names and addresses, and it's a crime to use an assumed name. Privately operated mail drops follow no such restrictions, and the operator's main concern is that the client pay his bill. A P.O. box contract runs for six months, while a mail drop rents for whatever the operator and client agree. The charge for a P.O. box of the smallest size is typically around ten dollars for each six-month period, while mail drops go for about nine dollars a month. Prices for mail drops vary widely, and there are special services available, such as remailing, at an extra charge.

The next category is the deceptive ad which promises more than the operator delivers. One common type, used over the years, is the one which promises a system of earning money which will make the client rich very quickly. Without telling the reader exactly what the system is, and often telling nothing at all, the ad promises him great success for a very minimal effort and investment. The sucker who sends in his ten or twenty dollars usually gets a booklet detailing an unworkable scheme, often involving a mail-order business.

Some ads promise to pay the reader. One, for a hair loss cure, promised to pay the reader five dollars to test the product.

Reading the fine print on this full-page ad revealed that the reader first had to buy the product, paying \$24.75, and the company would pay him five dollars only if he continued to use the product for sixty days and reported favorable results.²

The fake vacation coupon is a winner for the con man. A four-color ad appears, offering the reader a chance to win a free vacation in a contest if he'll send in the coupon. Each person who responds gets a letter telling him or her that he won the trip, an all-expense paid vacation in Hawaii or some other well-known place. However, there is a fee to secure the reservation and pay for mailing and handling costs. Those who send in the fee will find when the time comes for them to go on their vacation, some months later, that there is no trip, and the office has "moved," if it ever was there.³

Some people are leery of replying to a P.O. box. This caution is only partly justified, because private mail drops often have street addresses, which masks their true purpose. The reader may send in his money feeling a false confidence in the stability or legitimacy of the "company."

Another aspect that should be obvious is that in the real world nobody gives something for nothing, and this fact is obscured by cleverly worded ads that are designed to give the impression that Santa Claus has just arrived. Readers may find it hard to believe how much time and effort go into designing and wording the ads, the effect calculated to mask the fact that there is really no free lunch. One man stated that he usually took ninety days to design an ad, and that he'd go over it every day, word by word, in an effort to make it perfect before he inserted it in a publication.⁴

A variation on the vacation con was a group that operated under the name of an automobile club, and sent to purchasers of new cars letters offering them vacation gift certificates, good for all expenses, at various resort areas. The letter requested an eighteen dollar "service" fee.⁵

Yet another variant is the coupon book fraud, which may be for vacation areas or for local merchants. Some offers for books of "discount" coupons are legitimate, in the sense that the purchaser actually gets a book of coupons that the merchant will honor, but

others are strictly bogus, with the buyer getting a book of **counterfeits or nothing at all**. In any event, the buyer should be aware that merchants who “give” discounts are not seeking to lose money, and often jack up the prices to permit “discounts” and “rebates.”

Sometimes the fraud appeals to the victim's ego. One operator did not advertise, but used a commercial mailing list, sending each potential victim a letter telling him he was qualified for a listing in the local *Who's Who*. The letter informed the recipient he could purchase a copy of the book for a fee and that it would be sent to him upon publication. The swindler collected the money, but never had any books printed.⁶

Lonely-hearts clubs, computer-assisted or not, operate through the mails as well as face-to-face. However, some lonely-hearts victimizers offer spurious marriage proposals, extracting money in the process. One gambit is worked by a writer claiming to be female and played upon a lonely man. She offers to join him, if he'll send her money to cover her expenses in moving. She's always **a resident in another far-away state for this to work, and in reality** the writer may not even be female.

It also works the other way, with females being victimized by these gigolos-by-mail. Sometimes, the game is that the man asks the woman to invest in a business, or even to open a joint bank account.⁷

One widespread, but little-documented, area of fraud has to do with “swinger's” and other sexually-oriented clubs. The simplest ploy is for a “swinger's” magazine to have a classified ad section, in which readers place their ads seeking contacts. It's general practice for the listers not to have their names and addresses in the ads, but rather a box number care of the publication. The publication will accept and forward mail addressed to a box number, providing that the sender encloses a forwarding fee. In effect, the publication operates as a letter drop. There is no way to establish how many of the ads are legitimate and how many are spurious, inserted by the operator of the publication to stimulate traffic. The person who sends the letter off to a number at the magazine's office, not knowing who the ultimate addressee is, has no guarantee that the

person placing the ad, even if it is a legitimate ad, will want to answer.

The forwarding fee racket is only one of the scams that plague this sort of publication's readers. At least as common is the advertisement placed under false pretenses.

Some ads specify that the respondent must send a photo. In fact, some state boldly; "No reply without photo." In this context, "photo" means a photograph showing the genital area. Without a doubt, some ads are placed by sincere persons. Others are devices used by those who collect photos to add to their collections. Anyone who sends a nude photo with the initial reply to such an ad is taking a chance of having the photo wind up in some collection and perhaps being reproduced and passed around the country among members of the subculture that exchange such photos. Of course, there will be no reply.

One reason so many of those who place sexually-oriented ads use mail drops, even if they are legitimate, is because of the prospect of blackmail. Sending off a letter describing such personal details as sexual performances and practices to a stranger is risky at best, and if the recipient is running a blackmail racket, the outcome can be disastrous. Because of the underground nature of this sexual subculture, and the understandable reluctance of blackmail victims to report to the authorities, we'll never know the extent of this practice.

We can, however, make a guess that it is becoming less common. In recent years, a much greater proportion of the ads listed street addresses, phone numbers, and names. With the loosening up of sexual morality, and more widespread acceptance of practices that would have been cause for ostracism a decade ago, fewer sexual nonconformists find it necessary to hide their identities. A blackmailer would find it difficult to intimidate a person who does not care who knows of his or her sexual habits, and even may flaunt them, as by participation in a "Gay Pride" parade, complete with television coverage by Action News.

Nevertheless, there are many opportunities for deception with sexually-oriented ads. We can guess that this is a serious problem,

and even estimate the nature of the types of deceptions, by the exasperated phrases that appear often in such ads:

"No fats, fems, or drugs."

"No hippies or kinky stuff."

"Only sincere replies."

We can infer that some who respond to such ads are less than candid about their physical states or their practices. A person expecting a sexual contact from a response to an ad might not have formed an accurate impression of the respondent from the details revealed in the correspondence, and might be surprised to find that instead of a slim, youthful figure, the contact is aged and grossly overweight. Similarly, a contact seeker may be dismayed to find the second party has a drug habit.

Another area of trouble lies in what's covered by the word "kinky." While there are all sort of sexual preferences and practices, some are unusual indeed, and appear bizarre to the uninitiated. In the case of the sadomasochistic variants, they may seem not only bizarre, but are actually painful. Some who specialize in "genitorture," as it is known in the trade, will be quite forward about their preference. One such ad stated quite unequivocally: "Into heavy leather, S/M top....piercing and torture a specialty. Have full complement of toys."

There is nothing misleading about the wording of the fore-going ad, and anyone can tell what to expect. Others, however, are not so explicit, and misunderstandings result.

Some advertisers seek permanent relationships, and this can lead to complications, even when the participants are both sincere. When one or the other is practicing deception, problems inevitably result, and the only variable is how long it takes for the victim to realize that he's being had.

An ad that begins: "Seek young lady (or lad) to share home with older man...." will get all sorts of responses. It's inevitable that there will be an exchange of photos, which may be real or not. The ad may be a come-on placed by a photo collector, or it may be for the purpose of attracting sexually explicit letters.

Sometimes, the ad will go on to state the advertiser will help pay relocation expenses. This statement, in an ad, will attract a reply from every person out to make a dishonest buck. The game works the same way whether the relationship is heterosexual, homosexual, or of another category. The respondent sends a description that is appealing, and perhaps a photograph to back it up. It's an obvious fact that the letter may be totally false, and even written by someone of the opposite sex. Similarly, the enclosed photograph need not be of the letter writer. The respondent may indeed have collected some suitable photographs by placing a similar ad himself.

As the letter game develops, the "young person" pleads poverty, and may claim to be out of work. This can serve as an excuse for not having a phone or not contacting by long-distance. It also sets the stage for extracting money for "moving" expenses. The con artist, who "lives" several states away, has no job to tie him to the area, no great amount of personal possessions to add to the "moving" expenses, and appears to be a good deal for the older victim.

There are endless possibilities on the "moving expenses" game. Limited only by the victim's patience and gullibility, the fraud artist can extract several payments over several weeks' time. The first can be for "gas money" to enable the applicant to make the trip. After receipt of the first payment, the con man can come back and inform the sucker that his car needs repair, and to please send more money.

Yet another variation on the "moving in together" theme is a deception played by the placer of the ad. Posing as an older, established person, he places an ad claiming to seek a live-in partner, all expenses paid. Responding only to those in the local area, he'll meet them and initiate a sexual contact, possibly paying for a dinner along the way. The contacts somehow never seem to work out to permanent relationships, because the advertiser just wants to touch and taste, and is not seeking a permanent relationship, but a different partner every night.

In this sort of "affair" it often happens that the deception is not all on one side, and the initial contact need not come through the

mails. It's naive to believe that an attractive young person would be eager to start a relationship with an older one, at first sight unseen, out of love and devotion. Often, the real objective for the impoverished aspirant is simply a meal ticket.

Some relatively harmless ads in sexually-oriented publications are placed by "writers" who claim to be collecting "case histories" for an article or a book regarding some aspect of sex. Anyone who writes to them will find that these "writers" will ask them for very explicit details of their sexual practices, but will be very unspecific regarding when the article or book is due to appear, being unable to state who the publisher is. In fact, the "writers" are part of a very small sexual subculture that collects personally written pornography, preferring that to the hack-written porn that appears in commercial publications.

A variation on this theme appears in an ad that begins:

"Successful Free lance photographer...." and goes on to state: "Tell me your secret sex fantasy in your first letter -- and please include a revealing photograph of yourself." Apart from wondering why a "photographer" would be soliciting photographs, it's hard to tell what the motivation behind this ad is.

A variation of postal fraud that has nothing to do with sex is the sort of advertisement for "mercenaries" that appears in the "armchair macho" magazines, especially the ones that supposedly are aimed at "professional adventurers" and the like. The classified ad sections contain advertisements for "mercenaries," stating that there are jobs open for those interested in becoming mercenary soldiers, and offering "free" details. The advertiser claims to be a clearinghouse or employment agency for mercenaries, and the applicant finds out that, for a fee, he'll be told whom to contact for such employment.

Several angry letters protesting these "rip-offs" have been published in the letters-to-the-editor columns of these magazines, telling of the disappointing experiences that some applicants had had at the hands of these advertisers. Often, the fee would be twenty-five or fifty dollars, and the only reply would be an address in a foreign country. A letter to that address would produce no

reply, and follow-up letters to the “clearinghouse” would not be answered. Prosecution was hindered by the fact that some of these advertisers were in foreign countries, and we’ve already seen that prosecution across national lines is very difficult.

Another type of advertisement appearing in the “armchair macho” magazine offers instruction by mail in the various military skills needed to become a mercenary. There were no letters to the editors denouncing these rip-offs, and we can assume that those who sent in their money did get something back for it. The value of what they got is open to question. We’ve already seen the instruction in various store-front “martial arts” and “para-military and survival” schools is questionable at best, and that it simply isn’t possible to train someone to be a soldier of any sort in weekly Sunday afternoon sessions.

Those who employ mercenaries recruit from individuals who have seen service in an established elite unit, such as the SAS, Foreign Legion, etc., and who have combat experience. Any expectation that they would take seriously a certificate from a correspondence school for mercenaries is wildly optimistic, at best. Such instruction is in the same class as that offered by the mail-order schools for “detectives.”

There are endless variations of mail frauds employed, and the swindlers think up new ones, or new wrinkles on old ones, every day. Some of these fraud artists show great ingenuity, and often their efforts go well rewarded. Crime does pay!

NOTES

1. The Postal Inspectors will usually respond promptly to complaints of mail fraud, as the Post Office takes responsibility for the use to which people put the U.S. Mail. The Postal Inspectors originally were established to combat mail robbers, but their role has changed over the years.

The performance of the Postal Inspectors in contrast to that of the enforcement arm of the telephone company is painfully apparent to anyone who has had any dealings with both. The

frustration experienced by someone who tries to report something as simple as an obscene phone call is typical of what the telephone client can expect from the "security officers" of the phone company. In reality, the telephone company is not interested in what use or misuse a client may make of his telephone, as long as he pays his bill.

2. *Arizona Republic*, March 21, 1984.

3. *A Compendium of Bunk*, Carey and Sherman, 1976, Charles C. Thomas, pp. 127-128.

4. Author's interview with a mail swindler.

5. *Classic Mail Frauds*, Scot Tinker, Eden Press, 1977.

6. *Ibid.*, p. 31.

7. *Clipping The Flocks*, Scot Tinker, Eden Press, 1977, p. 16.

REAL ESTATE FRAUDS

Con artists selling worthless parcels of land and promoting various forms of real estate sight unseen have been with us for centuries. There is no documentation of the earliest such frauds, but we can assume that real estate swindles are truly classic. Probably the earliest ones in this country occurred during the last two centuries, which virtually covers the history of the United States. **Phoney gold mines were popular during the Nineteenth Century, after the gold rush.** The con man would sell a piece of land, or an actual digging, on which he claimed gold existed to be mined. In cases of skeptical buyers, the con man would make a small investment and buy some gold nuggets, with which he would "seed" the area and invite the prospective buyer for an inspection. "Seeding" a "mine" is a very convincing way to persuade a victim the land has value, and will fool anyone but an expert.

The Twentieth Century brought with it another variety of real estate fraud, the "vacation" or "investment" swindle. Florida was the site of a boom in land swindles during the 1920's, with con men buying swampland or tidal land and selling it sight unseen to buyers in other states. While this became a scandal at the time, new generations have come on the scene, and with them new swindlers, and the practice goes on, under different names and in different places.¹

Arizona was the site of many such frauds in recent years. The operators would sell their victims parcels of land that were out in the desert, almost inaccessible and with no fresh water or any utilities. Some of these parcels were on mountain peaks, but anyone buying them sight unseen would not know this.

While there are today some instances of swindlers selling property they do not own, faking the documentation and leaving town with the money before the victim finds out, this is outright, indictable fraud, which the smart operator tries to avoid because it leaves him wide-open to prosecution.²

Falsifying papers to a piece of land the swindler does not even own is possible, with little effort, but its success depends on

hustling relatively unsophisticated people, obtaining the money before they have time to check it out, and leaving as quickly as possible. Often, there won't be an outright sale, but just a request for a "deposit," or an advance on the "closing costs." The swindler convinces the victim he has a pressing reason for settling the deal quickly, and as the amount is not very great, and the total price very attractive, the victim pays willingly. The asking price can be extremely attractive, as the swindler is not selling the land and does, in fact, not even own it.

A variation on this theme occurs when the swindler notifies his victims they have "won" a parcel of land in a lottery or contest. He requests a nominal sum for "closing costs" on pieces of real estate that he does not own, or perhaps do not even exist.

With increased awareness of fraudulent land sales, and a tightening of laws pertaining to real estate transactions, the swindlers had to find new ways to sell property. Instead of the crude device of offering parcels that they did not own, they took to buying worthless land cheaply and inflating its value by selling dreams.

The operator would buy a large parcel of land, usually worthless but quite legitimate, and build a model home or two on it. Hiring an artist to draw up renditions of other homes, shopping centers, and recreational facilities, the swindler would promote this land to unsuspecting prospects. He would show them the drawings, and tout the property as a developing area with each piece of real estate appreciating in value over the next few years. In fact, the only appreciation would be the inflated price tag put on by the swindler himself, and any buyer who tried to unload his land later would have a hard time even finding another buyer, let alone collecting his price back.

Usually, the fraudulent sales presentations take place in a party-like atmosphere, with many people getting invitations by mail to attend the land offering. There will be refreshments, and the crowd will be laced by a few "shills," the swindler's confederates who will ostentatiously sign contracts for parcels and announce to the others they thought it was a terrific deal.

In some operations, there is an additional incentive. The operator offers his prospects the choice of an outright sale or an "opportunity" to get their parcels free if they find other buyers.

The operator may keep the ball rolling by renting some mobile homes and placing them on lots on the "development" to give the impression of growing sales. In some cases, he'll have his shills play the role of buying property from the first victims in order to develop a small corps of legitimate buyers who feel the "deal" is worthwhile and profitable, and will recommend it to their friends. Thusly, an operator who paid ten dollars for a parcel of land can sell it for several thousand dollars by investing in some minimal "improvements" and laying out some "front money" for his shills. In some instances, the wheeling and dealing can become quite convoluted, with the operator using other people's money and reaping his profit at each stage.³

The key to selling such real estate rip-offs is setting the atmosphere, and in some cases this preparation can be very elaborate. One source⁴ cites such a scene, in which the fraud artist approaches a couple on vacation, flatters them, gives them tickets to a show, and ends up by inviting them to a party on a yacht the next day. He tells them that the party is really a business meeting regarding a deal that need not concern them, and they should just enjoy the ride.

On the yacht, the master of ceremonies calls the meeting to order and begins to describe a land "deal" to a group of "investors." Some of them, the operator's shills, raise objections, but during the proceedings show they are convinced the "deal" is a good investment. Of course, the victims can't help but hear the presentation, and slowly get the idea that perhaps they, too, might profit from the "deal."

When the con man who approached them the day before sits down next to them and tells them that although he knows they are not interested in the "deal," it is a good investment for those who have enough money to buy the large blocks of land being offered. If they show the slightest flicker of interest, he continues to describe the virtues of the "deal" and the profits that an investor can earn. If he senses they are biting, he tells them although the

land is for sale only in large blocks, he'll talk to the man in charge and see if he'd be willing to release a small lot for his "friends." Inevitably, the man in charge is only too happy to release a small lot the couple can afford, and they sign a contract, pay the initial amount, and finance the rest.

Some of these operators seem to invest a lot of money in promoting their schemes. In some instances, they will even fly their intended victims to the site of the land, and despite the obvious fact the land is desolate, many victims buy on the strength of the con man's personality and the promise of development and appreciating value.⁵

Although driving or flying the marks to the site seems to be an unnecessary expense, there are certain advantages to this. Transporting the victims away from their familiar surroundings aids the con game, because it isolates them from friends and neighbors who might walk in to interrupt the proceedings, and forestalls them from picking up the phone to seek advice from a lawyer. Placing them in a group setting and using skills to manipulate the atmosphere is a clever use of the principles of group psychology, and we have already noted that con artists, although they may lack some formal education, are street-wise masters of practical psychology.

Turning to a fringe area, we find the "block-busters." They usually work in cities, concentrating their operations in neighborhoods that are changing in ethnic composition. Usually, the block busters are legitimate real estate agencies, promoting their business by using scare tactics.

In most cities, there are neighborhoods in which ethnic populations are entering. The block busters will canvass a block, telling each resident who answers the door that an ethnic family has bought a house down the block, or around the corner, and this will drive property values down. He offers to buy the house, usually for significantly less than the appraised value, and urges the owners to sell before it is too late. This process is exactly the reverse of the other sort of land swindle. Instead of promising an increase in value as an incentive to buy, the block buster promises a decrease in value as an incentive to sell.

Often the block buster is aided in his efforts by an ethnic family who actually moves into the area, for all of the other residents to observe. Inevitably, this will cause some of the homeowners to panic, and the real estate operator can play on their fears and pick up their property cheaply. He then resells it to other ethnic families, who are willing to pay his price because from their viewpoint, they are entering a better neighborhood than they left.

It's a misconception to think the only people who are taken in by land frauds are the stupid and unsophisticated ones. On the contrary, some frauds are designed to appeal to professionals. The "Land Paper" scheme is one.

Doctors, dentists, and other professionals often have money to invest, and indeed many of them are seeking tax shelters. The land paper artist does not sell land, but sales contracts to land at a discount. The con artist pretends to be from a well-known investment firm, and informs the doctor that it is holding paper on land which it wants to unload to make other investments. He promises a fat return, and a tax shelter. As an added inducement, he offers the doctor an option to buy stock in the company at a discount, adding that, although the company expects the value of its stock to go up during the next few months, even if the price remains the same the doctor will have made a profit because of the discounted purchase price.

If the doctor bites, he'll get payments from the company for a few months, and he may refer some of his fellow professionals to the company. Shortly thereafter, he'll find his dividend checks stopping, and when he attempts to contact the salesman he finds the office has moved, leaving no forwarding address. If he investigates further, he'll find the well-known company has no knowledge of the salesman or the land paper he sold the doctor.⁶

This is a variation on the Ponzi Game. The con artist knows that doctors have a lot of money, that they are interested in tax shelters and also earning more money, and that professionals in any community are a tightly-knit group, especially vulnerable to a Ponzi Scheme. If one bites, he'll recommend others, and the pack will follow the leader. In this respect, doctors are no more canny or resistant to victimization than their less-educated patients.

One type of real estate fraud that requires little investment from the con man and little time to carry out is the false rental. Basically, the fraud artist rents out property that belongs to someone else.

He gains control of the apartment or house by renting it from a legitimate landlord. He then advertises it himself, and rents it to all who are willing, establishing an occupancy date far enough into the future to enable him to swindle several other victims.⁷

A variation on this theme is to rent a property in a vacation area, and proceed to rent it out to many others. This practice solves two problems for the con man:

It permits him to rent the property sight unseen, to people who don't live in the area. This eliminates the possibility of the real owners seeing the ad in his local paper and becoming suspicious.

Usually, people rent a vacation cabin or apartment many months in advance, which gives the con man a comfortable margin during which he can rent the same property to as many people as he can inveigle.⁸

A legal version of the rental ploy is the "roommate" angle. The con man rents a luxury apartment with a lease that permits him to sub-let. He then advertises for a couple of girls to live in the luxury apartment, earning a small salary and free rental with the understanding that they would be "friendly." He then advertises for two men to share an apartment with two girls, at a rental that earns him a fat profit.⁹

A swindle that requires only a briefcase, some blank leases, and a convincing manner is the "new owner" swindle. The con man selects an apartment building and rings the doorbells a few days before the end of the month. He informs each tenant the building has a new owner. He explains the new owner has been concerned about the apartment manager, and he asks some questions about him, requesting that they keep the matter confidential because there was a possibility of replacing him.

At this point, the con man brings out a blank lease, and tells the tenant the new rent will be less than he had been paying. He requests the first and last month's rent, and leaves them a copy of the lease.¹⁰

The “rent skimmer” is another type who rents out property he doesn’t own. He works in at least two ways:

The first is to make a deposit on a house as if he were going to buy it. If he can get control of the keys this way, he can show the house to prospective tenants and “rent” it to them as if he were the real owner.

The first method works even better when the rent skimmer is a sales agent for a development. As the agent, he has the keys and control of the properties. As it often takes a year or more for all of the houses in a development to sell, the skimmer can rent out the unsold and unoccupied ones on short-term rentals, and pick up enough money to supplement his commissions very amply.

The second method is to gain control of the property by seeking out houses which are about to be foreclosed. When he finds one, he offers to buy the property from the harried owner at an attractive price, offering a very small payment as “earnest money.” The success of this scheme depends on the fact that there is usually a delay of several months between the initial transaction and the closing of a house purchase, and there is also a delay until repossession takes place on a foreclosure. The con man spends the time well, renting the house to as many as he can and disappearing with the money before the dates come up.¹¹

There is an endless variety of real estate frauds, and part of the reason they succeed is people place too much trust in a real estate deal, perhaps feeling because they are dealing in “real” property that is fixed and cannot be removed, they have extra security. This is often false, as what they are accepting in fact are some pieces of paper, not the real property itself.

NOTES

1. *A Compendium of Bunk*, Carey and Sherman, Charles C. Thomas, 1976, pp. 73-79.
2. *Big Time Operator's Manual*, Scot Tinker, Eden Press, 1977, p. 34.

3. Ibid., pp. 26-27.
4. Ibid., pp. 28-31.
5. *A Compendium of Bunk*, p. 74.
6. *Big Time Operator's Manual*, pp. 32-33.
7. *Professional Con Games, Schemes, and Frauds*, Carl Dorski, Roadrunner Publications, 1979, pp. 3-4.
8. *Big Time Operator's Manual*, p. 9.
9. *Clipping The Flocks*, Scot Tinker, Eden Press, p. 25.
10. *Short Cons*, Scot Tinker, Eden Press, pp. 30-31.
11. *A Compendium of Bunk*, p. 71.

STOCK MARKET FRAUDS

It might be accurate to say the whole market is a fraud, and indeed some people think so. The stock market, like the insurance business, is an example of a legitimate effort evolving into widespread fraud.

Let's take a quick view at how the market operates to understand the opportunities for fraud. The stock market is set up as a clearing house for the buying and selling of stock. Anyone who wants to buy and sell stock must do it through a broker, who collects his commission on the value of the stock he handles for his clients.

The values of stocks go up and down. An issue of stock may go up if the company wins a lucrative contract. It may go down if its sales are down. Rumors that concern a company may also affect the price of its stock. Trading in the stock, even if there is no apparent reason for the activity, will affect the price.

With this basic groundwork, we can see the opportunities for fraud. Firstly, we have the broker. He does not collect if his client's stock goes up or down, but only if the client buys or sells. He understands the more he can persuade his client to trade, the more commissions he will earn. Investors try to earn money on the stock market by buying a stock when the price is low and selling when it goes up. They sometimes seek advice from brokers, and it's a rare occasion when a broker will tell his client to stand pat, not to buy or sell anything. The broker always has a stock issue to push, something which "looks good" or "promising," and the broker is always assured of his commission, even if the client loses his shirt.

Brokers always try to stimulate sales, for that is the only way they can earn commissions. Some of them, even the big-name ones, operate "boiler-rooms," telephone sales operations in which their agents telephone people to try to persuade them to buy stocks. Those who bite are led on by dreams of riches from trading stocks, which the brokers avidly encourage. Clients may also be affected by the influence of the various books that appear with titles that follow the pattern *How I Made A Zillion Dollars In The*

Stock Market. These authors tell the same story: how they started out with very little money and, by their genius, parlayed the small sum into great wealth. They usually don't mention luck, preferring to take the entire credit themselves. Of course, the people who lose don't write books, as a title of *How I Lost My Shirt In The Stock Market* would not sell well.

Some brokers and investors make their own luck. They know hype and chain reactions affect the price of stocks, and they will quietly buy a stock when it is low, then plant something in the rumor mill. In doing this, they can exploit innocent clients by telling them the rumor they're planting, and in effect, using the client's money to "churn" the market, to stimulate activity. It usually happens that the price of a quiescent stock will go up as the volume of trading in it increases. This is called the "chain reaction." Brokers and investors out to "make a killing" will start the chain reaction by trading with each other. Others, attracted by the activity, will buy this stock, even though they don't understand exactly why there is such interest in this issue.

Some operators, who may be stockbrokers or executives of companies whose stock is on the market, try to profit by using "inside information," such as quietly buying an issue knowing that the price will rise when a forthcoming contract is announced. This is illegal, but people do it anyway. It is difficult for the Securities and Exchange Commission to prosecute if the operator covers his tracks even slightly, and a simple way to do this is to have a mutual aid agreement with another person. The operator tips off the accomplice when and what to buy, and the transaction does not have his name on it. It is easy to arrange a way of splitting the profits later. If the accomplice is an executive of another company, they can reciprocate favors such as these, making the arrangement untraceable, as there will be no suspicious transaction in the name of the one who has access to the "inside" information.

"Penny Stocks" are perhaps more popular now than ever. These are stocks in relatively small and little known companies, their prices rarely being over a dollar a share, which makes them affordable to working-class people. While investment in *any* stock is risky, because we don't know what the future will bring, buying

penny stocks is *very* risky, as the companies involved are new, have no “track record,” and the management may or may not be able to do the job. However, stockbrokers don’t really care about the future prospects of a particular stock. They seek to earn commissions now, in the present, and some operate “boiler rooms” to push penny stocks with people who have never played the market before.¹ It’s important to note that, although many of the penny stocks are those of real and legitimate, though struggling, companies, some of them are outright frauds. Some dishonest operators, not satisfied with the profits they can make through conventional stock market manipulations, seek to make a killing by buying a defunct corporation, using it as a shell, and promoting its stock. By setting up a boiler room operation, the operator can keep both the commission and the price of the stock.²

Sometimes, the stockbroker is the victim of a fraud. One way is for the fraud artist to place an order for the purchase of stock by phone. It sometimes happens that the broker, especially if it’s a busy day, will not check if the “customer” has an account. What happens next depends on whether the stock goes up or down. If it goes up, the “customer” shows up to pay for it, and then resells it at a profit. If it goes down, the “customer” does not show up, and the broker is stuck.³

Some overtly fraudulent investments are not offered on the stock market. Sometimes, the fraud artist will approach victims who obviously are wealthy, in a setting such as a yacht or country club, and by subtle play-acting, entice them into an “investment” in a new invention, design, or product. At times, the preparations for the scam can be very elaborate, and the fraud artist can string his victims along through several stages. Typically, the fraud artist, once he gets the initial investment, will wait awhile before asking for more money. He knows it is easier to wring money from someone by steps instead of in one big bite. The con man will announce there is a need for more money to provide “working capital,” pay “expenses,” etc. Sometimes he’ll be so brazen as to sell stock certificates, which may be those of a shell, or dummy corporation, or may be overt forgeries.⁴ It is easy to forge stock

certificates, and some swindlers have them printed by legitimate printers and use the phoney certificates as collateral.

Commodities are not stocks, but the commodities market works approximately the same way as the stock market. The brokers, earning commissions, try to persuade as many people as they can to trade as much as they can in the commodities they handle.

It gets to be really dangerous when the individual buyer does not buy a commodity outright, but gets involved in agreements to buy at a later date, called a "future." Sometimes, he'll buy an "option," which can get him into more trouble. The salesmen who push "options" and "futures" carefully gloss over the fact that the buyer is not buying real goods when he hands over his money, but simply pieces of paper. The one who falls for this "pitch" can find himself seriously hurt, and without recourse.

NOTES

1. *Big Time Operator's Manual*, Scot Tinker, Eden Press, 1977, p. 20.
2. *Ibid.*, p. 21.
3. *Ibid.*, p. 17.
4. *A Compendium of Bunk*, Carey and Sherman, Charles C. Thomas, 1976, pp. 107-114.

TANGENTIAL CONS

Tangential cons are deceptions not for immediate and direct gains, but as preparations for later criminal acts. A good example, used every day, is “casing the joint” by posing as a customer or salesman.¹

Eugene Villiod, French detective, says “opportunity makes the thief.” He also correctly points out that some thieves make their own opportunities. In real life, only the most raw and inexperienced thief commits his crime on impulse, without first carrying out a reconnaissance. Depending on the type of crime, the reconnaissance can be crude or sophisticated.

A solitary robber may just need basic information, such as the location of the cash register, the number of staff behind the counter, opening and closing hours, and the presence of any countermeasures, such as an alarm system. A burglar will be more interested in whether there is alarm tape on the windows, magnetic or induction alarms on the doors, the location of the control box, and whether the alarm rings a gong outside the store or a “silent alarm” that sends a signal to the police station or security service without alerting the intruder. Acting upon this information, he’ll plan to muffle the gong if there is one, or to cut the wires if it’s a silent alarm. Both robbers and burglars will want to “case” the surroundings, to plan getaway routes and note the frequency of police patrols.

There is little the store owner can do about this. He can’t refuse admission to his store, although in some unusually rough **neighborhoods, liquor stores are barred and sell only through a teller’s grill.**

Better organized burglars and robbers use an advance man, a specialist who does not participate in the act itself but who seeks out and presents information about the target. He may also be a planner, devising the mode of entry and the subsequent events. For this service, he gets a share of the “take.”

Advance men are specialists, not strong-arm men, and they develop special skills to supplement their eyes, ears, and common

sense. They are, in a sense, con men, because often they play a role as they gain access. The advance man may pose as a salesman, inspector, or service technician in order to scout the premises.

Sometimes he's not playing a role, but really is such a person. A minority of such mobile people, with criminal contacts, know they can earn extra money with no risk by passing on "tips" about likely targets to the right people.

There is no defense against this type of scout. He is the person he claims to be, and checking with his employer will verify this. The typewriter repairman or telephone installer comes onto the premises with the express permission of the person who ordered the service, and his cover is unbreakable.

The complex technology of the Twentieth Century has not only increased the number of crimes, but has made carrying them out successfully easier for the criminal. The same telephone that permits a citizen to report a crime promptly to the police enables the burglar to check if anyone is home before he approaches. The increased affluence which has more people than before living in one-family houses on fenced-off lots for privacy permits the burglar to work unobserved by neighbors.

House and apartment dwellers are also targets for criminals. The advance man can be a salesman, bogus or legitimate, who under the guise of selling his product or service often gains admission to the home, where he can scout for items of unusual value that would make an attempt worthwhile. In conversation with the resident, he can elicit information that is valuable to a burglar. On the pretext of visiting the bathroom, he can scout another room or two. One who poses as an "inspector" can have the run of the house.

Burglars, although sometimes armed and dangerous, usually don't want to run into anyone when they're doing a "job." They want to know when the residents will be away from home. As a last minute check, they'll phone the target. If nobody answers, they know the resident is either out or in the bathroom. An unlisted number is not necessarily protection, as the advance man may have had the opportunity to read the number from the phone while in the home.

As a final check, the burglar will scout the premises before his final approach, checking if there is a car in the driveway or garage, or if there is noise coming from the home. The final step is to ring the bell. If, after several rings, nobody answers, he'll know the "coast is clear." If someone does come to the door, he'll pose as someone who rang the wrong bell, or if the hour is appropriate, a salesman. The stereotype of the criminal with a mask and a blackjack sticking out of his pocket will not fit him.

Telephone "surveys" can be subterfuges for tangential cons. One example is the car-theft-to-order ring. In states in which motor vehicle registrations are not accessible to the public, the scout for the ring has the choice of riding the streets until he sees a car in demand, or phoning until he finds one. He'll pretend to be making a survey on car care, asking questions about the maintenance the car has received, and of course the make and model. For his select customers, he'll want a "clean" car, one that has been well-treated, and he'll want to know where to find it at his convenience. Riding the streets means he strikes at targets of opportunity, forced to steal them where he finds them. While there are car thieves who use inertia hammers to rip out the door lock, the high-class "car-to-order" thief does not want to damage the car, and prefers to make off with it at his leisure.

An unusual method of "setting up" a victim for a robbery involves a large cash payment. When this criminal wants a new car, he buys it for cash, bringing the money to the sales office but first tipping off his partner. As soon as the buyer pays for the car, a perfectly legitimate transaction, the buyer leaves and his partner drops in to rob the dealer. They later split the money.²

NOTES

1. *Crooks, Con Men, and Cheats*, Eugene Villiod, Gambler's Book Club Press, 1980, pp. 88-98.
2. *Professional Con Games, Schemes, and Frauds*, Carl Dorski, Roadrunner Press, 1980, pp. 22-23.

TECHNOLOGICAL FRAUD

Certain aspects of high-tech fraud would require a book of their own, but we won't concern ourselves with the intricacies of computer crime and other massive complexities because most of us won't even get close to them. There are some ways in which cheats and con men do use bank computers to defraud others, and we'll look at one of those ways now:

A plastic, magnetically-imprinted bank card, designed for electronic banking, can be used as an adjunct to a fraud. In most systems, a deposit at an electronic teller will show immediately in the balance on the printed slip, although the money won't be credited to the account until a human teller can open the deposit envelope and verify the amount. The cards can also call up a statement of the account balance, even without a deposit. This weakness can make it easy for a con man.

The swindler, determined to take advantage of this situation, goes to the electronic teller after the bank's closing, and makes a "deposit" of a large sum. The envelope he puts into the slot is empty, however, but this does not register with the computer. This is the key to getting away with a piece of merchandise and leaving only a small deposit. If the item in question is a car, for example, the fraud artist can take the seller to the electronic teller and show him the balance in his account of fifty thousand dollars, as proof of ability to pay. If, as the smart con man will arrange, the meeting takes place after banking hours, there is no way the victim can determine he's being set up. The fraud artist makes off with the car, and the victim waits and waits and waits.

Anyone who carries a plastic card, whether it be for banking or straight credit card, should be aware that some thieves specialize in stealing and fencing these precious pieces of plastic. Similarly, a businessman who deals with the public should be aware of the procedures for handling the threat of stolen, expired, or forged credit cards. Some credit card artists can evade being traced because they know that, until the "hot list" of lost and stolen cards comes out, the merchant is not required to check with the

company unless the amount of the purchase exceeds a certain amount.¹

The limits on credit card fraud are sky-high. A swindler using a stolen or lost credit card, can even charge amounts over the limit, as when stopping at a hotel. The hotel won't verify the amount until the final bill is settled, and the swindler can quietly leave long before then.²

The swindler who is in collusion either with the legitimate "owner" of a plastic card or with a dishonest merchant can, by simple falsification, take in a lot of money or goods in a very short time. The partner simply hands over his credit card to the swindler, delays notifying the home company, and meanwhile the fraud artist uses the card profusely, secure in the knowledge that he's in no danger of even being challenged for forty-eight hours. At the end of that period, the partner reports his card "lost," knowing the law makes him liable for only the first fifty dollars.³

A small-time rip-off, more common now that most deposit slips are magnetically imprinted, is for a fraud artist to open up a checking account, or an electronic savings account as a first step. It's vital for him to have a means of withdrawing money from this account without showing his face in a bank office, for the risk of detection is great enough to make this very dangerous.

The second step is to have many duplicate slips printed, without a name but with the magnetic number on the bottom. The fraud artist then goes around to several bank branches and places these slips in the compartments at the customer service tables.

Inevitably, some customers will notice the discrepancy. Also, inevitably, some will not, and the swindler who keeps his plastic card handy to make withdrawals as the money flows in and before the account is stopped can collect these intentionally misplaced deposits.

Turning to another currently popular type of fraud involving a computer, we find the "computer-dating" services. These are just variations on the old lonely-hearts clubs, but with a modern twist that is real at times and outright false at others. The program works in this manner:

The operator sends each applicant a "computer form" containing a large number of questions, some very personal. Allegedly, the answers will be "analyzed" by a computer to determine the personality type, and the applicant will be matched by the computer to the most compatible personality in its memory bank.

There are several things wrong with this basic idea. One is that matchmaking is not a science, but an art, and there are no scientifically valid criteria for matching people by computer. Even if the test handed to the applicant is designed by a "psychologist," and even if the "psychologist" is real, the test is not validated through the use of control groups comprising thousands of testees, an essential before a test can be considered valid.

Another trouble area is the way the "computer dating service" is presented to the applicant. The operator promises the applicant that he or she will be matched with intelligent, attractive members of the opposite sex. According to the operator, only the best people, upwardly mobile and very well-off and sexy, form the dating pool. The people who are taken in by such operators perhaps do not stop to think it out, and do not realize that the truly superior group of people described in the brochure does not need a computer or any other kind of dating service, that they have no trouble finding dates on their own.⁴

More than any other, this is an unfinished chapter. Technological improvements bring new frauds into the realm of possibility constantly, and new techniques of access and communication bring with them new versions of fast-moving fraud.

NOTES

1. *The Fraud Report*, 1977, Financial Management Associates, 3824 East Indian School Road, Phoenix, AZ 85018 Section 2, p. 5.

2. Ibid., Section 2, p. 7.

3. Ibid., Section 2, p. 8.

4. *A Compendium of Bunk*, Carey and Sherman, 1976, Charles C. Thomas.

TELEPHONE GAMES

The telephone is a modern convenience, but it would be only a minor exaggeration to call it an instrument of evil, in some situations. There are many frauds that depend on the telephone for success.

We start with the classic and simple fraud, whereby an individual using a pay phone gets a free call. The person inserts a coin and dials "Operator." When the operator answers, the game goes like this:

"Operator, I was trying to get my number, 123-4567, and I heard a couple of clicks and the line went dead. I lost my coin."

"I'm sorry. I'll try it for you. Give me your address and we'll send you your coin back in the mail."

Another game to play with pay phones is to tape record the sound of coins dropping, using a small and portable machine. When calling long distance, playing the tape for the operator will fool her into thinking that there are actually coins deposited.¹

There is a category of people called "phone phreaks," who circumvent the phone company's safeguards because they are talented in electronics and construct devices to fake control tones that switch long-distance lines, or even by having them billed to another party. In some instances, the phone phreaks are able to break into supposedly secure lines belonging to the government and route their calls through them.

Annoying as these people may be to the telephone company, we can't get very indignant about their actions because firstly, they're more fun and games than victimization. Secondly, it is hard to get excited over a corporate giant, such as the phone company, losing nickels and dimes to individuals.

It's another matter when criminals use the telephone to victimize the innocent. We can recognize the distinction, although the phone company pretends that it does not exist, and treats con artists just as it does other customers. This practice seems bizarre when compared to that of the Postal Service.

The Postal Service keeps a staff of Postal Inspectors who investigate mail fraud. By contrast, the phone company, another medium used by fraud artists, uses its security operatives mainly to oversee the security of its physical facilities and to pursue clients who don't pay their bills. This is why, although mail fraud is big business, telephone fraud is gigantic.

The classic example of telephone fraud is the "boiler room." This is a room full of desks, phones, and people who run down lists generally taken from the telephone directory and pitch the people who answer. Sometimes the boiler room is legitimate, as in selling tickets to the fireman's ball. More often, there will be an element of deception. One pitch went like this:

"Hello, Mr. Smith. This is Mr. Jones from the Brooklyn Children's Shelter. In cooperation with the Daily Pitch, we're asking people to help the Brooklyn Shelter. If you subscribe to the Pitch the Shelter will get full credit for that, and you'll be helping needy kids."

In reality, this was just a device to sell newspaper subscriptions, and the "Shelter" got, instead of "full credit," a donation of 25 cents for each subscription.²

Phoney charities are classic devices for conning people out of their hard-earned money, and they work on the phone as well as they do face to face. They lend themselves well to boiler room operations, because the con man can hire innocent people to make the pitches for him. Not having polished and professional salesmen make the sales talks is not a handicap in charity frauds, because sales "pros" would be out of place in such a setting.

For products and services not claiming to be charitable, the pitches can be ingenious indeed, and the telephone techniques literally far-reaching. Boiler rooms, like legitimate businesses, use WATS lines to obtain low-cost direct dialing across the country. A crew working in New York can canvass the country systematically. A recent development is the computerized telephone dialer, which dials one number after another until there is an answer, then plays a taped sales message to whoever is listening, and signals a human salesman if the person is still on the line after the end of the

message. This device saves a lot of salesmen's time, and wastes a lot of other people's.

Sometimes the victim has a chance of recognizing the fraud because the approach follows well-known patterns. A voice on the telephone which announces that it is making a "survey" is usually the beginning of a sales pitch. A caller who tells his victim that he wants to give him a "free gift" is also trying to sell something. Sometimes there will be a "quiz," with an easily answered question that then "qualifies" the victim for the "prize" or special "low introductory offer." Some of the varied approaches used are truly ingenious.³

A particularly brazen fraud, operated out of a phone booth, was the "Cadillac" game used by a man who passed himself off as the producer of a famous television show. He'd ask the victim to appear on the show, and added that part of the fee for the appearance would be a Cadillac. He told the victim that a representative would be in touch to help them select the car.

Several days later, a man with the proper credentials would show up, and tell the victim that of course, all expenses would be paid for the appearance on the show, and that he could select his Cadillac right away from some brochures. If necessary, they'd go to the local Cadillac agency, where the victim could examine the cars before making his selection, which would be ordered through the television production company, not the local dealer.

The "representative" would then carefully tell the victim that, while the producer could legally give away the prize, the law required that the sales tax and license fee be paid by the person receiving it. He'd extract the amount from the victim, who would never see him again.⁴

Answering the phone nowadays can be a hazard, not so much to the health but to the wallet. The use of the phone for sales pitches and for fraud is now so great that some people think of it as "pollution."

NOTES

1. *Professional Con Games, Schemes, and Frauds*, Carl Dorski, Roadrunner Publications, 1979, p. 27.
2. Personal knowledge of the author.
3. *A Compendium of Bunk*, Carey and Sherman, Charles C. Thomas, 1976, pp. 46-47.
4. *The Fraud Report*, 1977, Financial Management Associates. Section 5, pp. 11-13.

THIRD-PARTY CONTRACTS

An interesting opportunity for the fraud artist, and a great danger to the consumer, is the "third-party" contract. This means that when a customer buys an article on credit, the credit being supplied by a party not connected with the seller, the lender is not responsible for the quality of the item and has the right to demand payment.

While the law in this regard varies from state to state, and some states have certain consumer protection laws that affect third-party contracts, the procedure is usually the same. The customer buys an item on credit, using a credit card, securing a loan from a finance company, or a mortgage from a bank. He is then obligated to make payments, regardless of the conditions of the sale or the item purchased. Any questions regarding the quality of the goods or the terms of the sales contract do not involve the creditor, and are strictly between the seller and the buyer.

Third-party contracts are daily occurrences, and often do not pose any problem at all. It's also important to note that when there is a problem, it is often possible to resolve it without concern over the terms of payment.

When a customer buys an article from a reputable outlet, and pays for it with a bank credit card, not a store charge account card, he's obligated to pay the amount due. When there is a problem with defective merchandise, the reputable outlet will either repair or replace the item, or will take it back and issue a credit memo, cancelling the original amount charged to the credit card.

The interesting opportunity for the fraud artist is that in selling a large-ticket item, he can obtain his money quickly, with the customer footing the bill for the finance charges, and in fact if the seller acts as an agent for the credit company, processing the paperwork, he often earns a small commission from the lender on top of his profit.

With the money in his pocket, the fraud artist can leave town. The defrauded customer is left "holding the bag," obligated to make the time payments. In the cases of fraud artists who stay at

the same location for years (used car lots are good examples) the fraud artist knows that the customer has, through the credit source, already paid him and cannot hold out payment to enforce his demand for satisfaction.

The danger for the customer is obvious. As we've seen, he's left holding the bag, and often has no recourse. While he is also left holding the bag in small transactions, the amount of money lost is not as painful. Being obligated to make payments on a car that doesn't run, however, will often prevent him from getting credit to finance one that does, and if he needs a car for daily use, he'll be in deep trouble.

In the case of a fraud artist who has left town, the effects are often more far-reaching. Not only is pursuit and apprehension of the fraud artist more difficult, but the customer may be left to deal with a contract upon which the vendor has defaulted. An example is when the customer buys an appliance, such as a sewing machine or water softener, and the transaction includes either a warranty or a service and maintenance contract. Although the customer will not get the service called for in the contract, he must continue to make the payments.

What we can learn from this is clear: Apart from the extra thought that must accompany any purchase which involves a large amount of money, the customer must also be wary of any that call for third-party contracts because of the danger of that extra degree of victimization. Except for states which have provisions in their consumer-protection laws that cover third-party contracts, the defrauded customer has no recourse.

STRIKING BACK IS HEALTHY

In recent years there's been much attention paid to the plight of the criminal, and in the process the victim has been forgotten. It's easy to overlook the fact that the victim loses in two ways, materially and psychologically.

Whatever the nature of the crime, police and psychologists have observed victims undergoing a psychological upheaval that, in some instances, can be very severe. If the crime is violent, there is mental as well as physical trauma. Even in the absence of severe physical injury the victim suffers the after-effects of anxiety and fear. In many cases, there is a feeling of helplessness, which is the beginning of depression.

The victim of fraud has a mental burden to bear, although he almost never has to cope with violence or even the threat of violence. Yet, he has lost, and the circumstances of his loss make it more depressing. The victim of a burglary may be very unhappy at the loss, but the thief, operating by stealth, is contemptible. The fraud victim has to live with the knowledge that he's been outwitted. The fraud victim, strangely also, does not get the sympathy from friends and family that other victims do. Even the victim of rape will find sympathetic faces, people who understand that it might have happened to them.

The fraud victim has no such support. He may quite rightly feel that the attitude of others is: "He let himself in for it, the jerk." This is a blow to the ego, and intensifies the victim's problem.

We've seen that, in crimes of violence, the law is clearcut and the police will make an effort, although the clearance rate for crimes is discouragingly low, and the net result is that only one or two percent of criminals go to prison. In cases of fraud, the police may not even recognize that there's been a crime committed, telling the victim: "It's a civil matter." This leaves the victim high and dry, not even knowing where he stands.

In all crimes, punishment of the criminal is psychologically satisfying to the victim. If it is direct and personal retribution, it satisfies the need to hurt the criminal as badly as the victim was

hurt. If it is retribution by the state, at least there is the satisfaction that justice will prevail, that it is a well-ordered world in which the bad guys are punished.

When, as so often happens, the criminal is not caught and punished, it leaves the victim angry and frustrated. He's justifiably angry at the wrong that was done to him, and he's frustrated by a system that doesn't seem to work. Reading of the many other cases in which criminals get away with it reinforces and intensifies the feeling of helplessness.

This section is aimed at the victim and potential victim, in an effort to help both in protective means and the means of striking back. It's mentally healthy to be able to protect oneself. It's mentally healthy to want to strike back after being hurt.

We'll consider three areas: passive defense, in which we look at simple methods that are very effective for the time and effort involved, active defense, and counter-attack.

PASSIVE DEFENSE

Passive defense consists of measures you can take, without much effort and at no cost, to reduce your vulnerability to fraud. The principles are well-known, and the major disagreement is on how far to go.

Keeping a low profile is an obvious first step. This means blending in with the crowd and not standing out as a potential target for a fraud artist. Keeping a low profile also means not flashing a roll of money, not dressing exceptionally opulently, not having an obviously expensive brand of luggage when you travel, and perhaps even making it a point not to travel first class. Custom license plates, like expensive cars, are out. If you look prosperous enough, someone might think you're worth kidnapping.

Awareness of the basic frauds and some of the modern variations is the next step. Learn to recognize the basic con games and know the roles that con men and their accomplices play. It is impossible to keep up with all of the new wrinkles in fraud, partly because no true encyclopedia of fraud exists, and it's hard to see how anyone could compile one without its becoming obsolete before it got into print. Still, you don't need to know it all, just enough so you'll be aware of the scams that someone might pull on you.

While some authorities advise being withdrawn and not talking to strangers,¹ carrying out all of their recommendations would result in a totally closed-in lifestyle. It is not necessary to go that far. It is important not to be too free and easy with strangers, and to pick your associates carefully. Being aware of the fact that "sheet writers" and fake bail bondsmen frequent conventions and vacation resorts, it is prudent to be wary about discussing personal affairs with recent acquaintances. It's not necessary to distrust all strangers and treat them with suspicion and coldness bordering on hostility. You need only to be aware that seemingly harmless details you may divulge about yourself can be used against you by a fraud artist.

Gambling with strangers is a no-no. The floating crap game or the “friendly” game of poker in a hotel room that suddenly turns ugly are two prospects that are easy to avoid.

Lending money to strangers is in one sense the same as lending it to a friend. It boils down to the question, “How much can you afford to lose?” Most of us have been “stiffed” by a friend who simply “forgot” to pay back a small loan. With a stranger, no matter what the story, we have no way of knowing at the outset whether the borrower is for real or just another slick deceiver. A decision we can make in advance, and which will cover all circumstances is the amount we’re willing to lend. We must be prepared for the possibility that our humanitarian impulses will lead us into trouble, and be prepared to cut our losses.

Another aspect of passive defense also has to do with mental preparation. It’s important to develop a certain skepticism and to understand that if an offer sounds “too good to be true,” it probably is. There really is little chance of getting “something for nothing,” or “striking it rich.” Even if there were, why would a stranger share his newly-found secret of wealth with you? Because you’re a nice guy? There are adults who succumb to the charming, smiling stranger who’s going to make them wealthy, although if you were to ask these adults if they believe in the tooth fairy, they’d feel insulted.

Some of the precautions you can take serve double-duty. Not widely spreading the news of your impending travel not only forestalls some of the away-from-home schemes, but also helps to avoid being burglarized while away.

Some precautions present problems. Not having your name and address on the outside of your luggage helps to prevent some swindles, but it also prevents or impedes its return if lost. Having identification on the inside only is largely futile, as a baggage thief will surely open the case.

While it’s going too far to distrust all strangers, there are some cases in which precautions are prudent. Picking up hitch-hikers is not dangerous most of the time, but there’s always the occasional one who’ll make you wish you’d never seen him. Each person has to assess the risk for himself.

Never letting a stranger into the home is another yes-no-maybe situation. While it's obvious that taking a hitch-hiker home with you, no matter how nice he seems or how sorry his tale of woe, is often the prelude to trouble, it's impossible to generalize more than that. The person who knocks at your door and asks to use the phone may be a criminal or someone in trouble, and it's not always possible to follow the conventional wisdom and make him or her wait outside while you place the call for them. In bad weather, few people can resist letting in a stranger who claims that his car stalled.

There are, of course, repairman and "inspector" types who want to get into your home, and checking credentials and verifying identities with their central office is a wise precaution. In any event, you will know whether or not you sent for a repairman.

In doubtful situations, try to pay by check, as many a con man will find a check a problem if he's seeking just quick cash. A check also gives you the opportunity to stop payment if, after checking or thinking it over, you decide you're in for a fraud. In any situation with someone asking you for money, unless it's a transaction you've initiated, be careful. Accepting a C.O.D. parcel, paying off someone's debt, buying a subscription or putting a down payment on a piece of property are ways some frauds start.

Finally, if you're one of the millions of Americans who may let him or herself into a sexually compromising situation, be very careful, not only of your partner, but of the situation as a whole. The care you need to take depends on your situation and your habits. If you're a husband seeking some fun on the side at a convention away from home, and you have an understanding wife, your situation is not as acute as that of the homosexual who works as a schoolteacher and who picks up young male prostitutes in the park.

Anyone with sexual habits that are either illegal or which may cause embarrassment if discovered must learn great discretion. As with other threats, there is no perfect defense, and the sexually deviant person will always be at least minimally exposed to risk.

SOURCES

1. *Complete Security Handbook*, Anthony B. Herbert, 1983, MacMillan Publishing Co., Inc., 866 Third Avenue, New York, NY 10022.

This book covers all aspects of personal security, but the precautions listed, if followed as closely as the author suggests, lead to a very restricted and fearful lifestyle that few people would willingly adopt. Most of us are willing to accept a slightly higher risk for more freedom.

THE ROLE OF THE POLICE

There are two main reasons fraud artists have such success:

1. *Public attitudes.* Most people tend to think of crime as they see it on TV: shootouts, car chases, and unrelenting violence practiced by desperate or psychopathic criminals. The news media help this image of violent crime, faithfully reporting every rape and murder, giving the bulk of front-page space to the criminal who kidnaps and murders a baby, not the smooth-talking fraud artist. The public remains unaware of the greater volume of "white collar" crime, and being unaware, is more open to exploitation.

2. *Police attitudes.* The police feel most comfortable with a straightforward violent crime, one in which there is no need to deal with such intangibles as pattern and intent. They are geared to overwhelm violence with superior force, and this shows even in their equipment. Police officers carry revolvers, but few have even a pocket calculator as part of their equipment. Some of the larger departments have a fraud or "bunco" squad as part of their detective bureaus, but numerically they are few, although non-violent crimes far outnumber the violent ones, and are more profitable.

The police are wary of entering the field of civil disputes. It has happened many times that citizens and businessmen have tried to use the police as a collection agency to collect money due them. Police know they do not belong in matters that properly belong in civil, not criminal, court. In many instances, they do not even recognize a fraud scheme as being one.

The attitudes on the parts of both the police and the public form a combination that greatly lubricates the way for the fraud artist. When a citizen does make a complaint (and many do not) the police reaction is likely to be: "That's a civil matter." Often, it is not clear to the police that an incident forms part of a pattern, unless several victims report the incidents.¹

Allied to this is the difficulty of convincing some people they're letting themselves be victimized. For example, there was an incident of a woman who phoned the fraud squad regarding a

chain letter she'd received. The detective who spoke to her spent some time explaining that chain letters are money-making schemes only for the ones who start the chains, and her chances of becoming rich were nil. He added that participating in a chain letter was a misdemeanor, but she remained unconvinced.²

Reporting the incident to the police often is not enough to bring the affair to a successful conclusion. To obtain a prosecution and conviction, it may be necessary for the victim to take the time to testify in court. If you've been victimized, you may find this difficult, for several reasons:

1. The place where you're required to testify may be quite far from your home, as many con games victimize people who are away from home on vacation or at a convention. **Sheet writers and phoney bail bondsmen, for example, do this.**

2. You may feel the effort required is not worth it. If you've lost only one hundred dollars, for example, and you have to take a lot of time off from work to testify, the effort would be out of proportion.

3. Coming out into the open may be personally embarrassing for you. If you've been a victim of the badger game, for example, reporting the incident will mean that you have to face the publicity, and the more serious your role the more harm this can do to you. Many victims, such as homosexuals and married men, feel they can't take the heat. Fraud artists count on this and it often happens the police will know of the operations of a fraud artist, but won't be able to find any people willing to cooperate in the prosecution.

4. Conviction rates are low. Part of the reason is, in many states a technicality of the law prevents the prosecutor from mentioning the defendant's criminal record to the jury, although the judge will know of it and take it into account in sentencing. The reason for this wrinkle in the law is that knowledge of a prior conviction may prejudice the jury in considering guilt or innocence in the current case. While this may be valid for other types of crimes, it is counter-productive in fraud cases, where there is so much deception involved and where an important part of the case is the

pattern. It's easy for the fraud artist to convince a jury that "it was just a misunderstanding," in one instance, but if there is a long record of such "misunderstandings," he will find it much harder to persuade the jury to believe him.

5. If you're the victim of fraud, you may decide the police will not be as helpful as they would be in other types of crimes. Hard reality is much different from the illusions some people carry. The real police, unlike TV cops, do not always get their man, and the picture becomes even more discouraging when they don't seem to be making even a reasonable effort. For example, in some cities, the police will not send an officer to investigate a burglary, instead taking the report by telephone.

There is one exception to the disappointing performance of the authorities. The victim of fraud can retaliate by sending the "Gestapo" after the fraud artist. Some Americans refer to the Internal Revenue Service as the "Gestapo," and there is a certain resemblance in one respect: both are terribly efficient. The original Gestapo derived its frightening reputation not so much because of brutish sadists who beat the arrestees mercilessly, but because Gestapo officers were mostly brilliant men who were good at their jobs. The Internal Revenue Service, despite much bad publicity, is staffed largely by dedicated people, and in the case of a fraud artist, you can put them to work for you.³

The IRS has a program of rewarding informers, sometimes called the "Turn in a friend" program, in which it pays cash rewards (taxable, of course) to people who tip them off to those who are evading income taxes. Unlike local police, the IRS is a nationwide agency, and has formidable investigative resources. Also, the IRS will devote a great deal of manpower and effort to getting a conviction, mainly to make examples of tax cheats and show others they can't get away with it.

If you have reason to believe the person who defrauded you is not declaring his income, and if you can pinpoint him to the IRS, you can give them a "tip" which will start an investigation. The IRS will pick up the ball and you probably won't have to testify in court, as the prosecution will be for evading taxes, not victimizing

a specific person. You could even make some money from the affair, which may or may not pay you back for what you've lost.

NOTES

1. *Fraud Investigation*, Glick and Newsome, Charles C. Thomas, 1974, p. 11.
2. *A Compendium of Bunk*, Carey and Sherman, 1976, Charles C. Thomas, pp. 7-8.
3. *Ibid.*, pp. 91-92.

ACTIVE DEFENSE

Active defense is just that — active, direct means of defending yourself against a fraud artist, but stopping short of serious retaliation. Although in principle the distinction between defense and counter-attack should be very clear, in real life it is blurred, and there's an element of counter-attack in some defensive measures.

Let's start with the mail. Each day brings its quota of junk mail, with the fabulous free offers and announcements that you've just won a contest. Often, these littering letters have business reply cards or envelopes included. Instead of throwing them all away, seal and mail them. The recipient will have to pay the collect postage on each one.

Moving on to the phone, it's a good idea to ask who's calling each time the phone rings. Instead of allowing a salesperson to waste several minutes of your time with a "survey" or other nonsense, ask immediately for the name and company affiliation. Don't be shy. If the offer is for a "free gift," tell the person to send it in the mail, that it's not necessary for you to be at home to receive a gift. That usually stops them cold. If there's only a taped message on the other end of the line, you'll know and be able to hang up.

A telephone answering machine is a good way of screening out junk calls. Most salespeople will simply hang up when a robot answers them, not wishing to waste their time. Keeping the machine on, even when home, and using the "monitor" function will save you the need to answer calls you don't want.

A simple tactic is to hang up, without warning and without saying "goodby." You'll find it easier to ignore your impulse to be polite after the salespeople have interrupted your supper for the fourteenth evening in a row, and you'll find it hard not to hang up with an obscenity.

The essence of good tactics in active defense is simplicity. There's no need for complicated plans, which sometimes are more trouble than they're worth.

Coping with panhandlers, whatever their come-on, is simple. Tell the panhandler you left your wallet home that day. This will work especially well on the office panhandler who comes around with his tale of having lost his wallet and the contents of his briefcase.

The quickest way of coping with the “pigeon drop” and similar scams is to suggest that the best thing to do with the “lost” item is to turn it in to the police. You’ll be surprised how quickly he’ll lose interest in you.

The simplest turn-off for any money game, hot goods scam, or any scheme to extract money from you on the spot is to say that you don’t have enough money with you. If the con man wants twenty dollars from you, tell him you only have twenty cents. If the con man suggests that you go to your bank to withdraw the amount, tell him that your bankbook or plastic card is at your lawyer’s, as there was a problem that needed straightening out.

Looking at the simplest methods, always get up to go to the kitchen or bathroom when you’re watching TV and the commercials come on. They’re all lies, anyway. Why waste time watching even for a minute?

Learn to use time to your advantage. As we’ve seen, the majority of con men are hit-and-run artists, straining to make a quick buck and leave town. They’ll try to “hustle” you, to press you to act immediately. The best thing you can do, if something seems not quite right, is to temporize. Playing for time will work in almost any situation. To select an extreme and ridiculous example, if you’re a witness to the “flop” game, in which a “doctor” takes up a collection for an undernourished person laying on the sidewalk, it’s easy to say: “I left my wallet home. Give me your card and I’ll send you a check.”

Using your lawyer, whether you really have one or not, will save you a lot of grief and give you an impregnable position from which to resist high-pressure tactics. Whether the deal is a car or a piece of real estate, if you think something’s wrong, dig in your heels and say flatly: “I never sign a contract without showing it to my lawyer.” If you’re fifty miles out in the boonies, looking at worthless land, the same isolation the con artists see working for

them will work for you, if you insist you always show legal papers to your lawyer before signing. At least, this tactic enables you to play for time. If the deal is valid, it will surely still be there tomorrow. If the salesman insists this is a once-in-a-lifetime opportunity, that's almost a sure tip-off it's a fraud.

Knowing your prices is basically passive defense, but using the information actively is another matter. Door-to-door sales people will often try to sell you something at an exorbitant price. In principle, the salesman should never have gotten in the door, but a relative may have admitted him and now you find him pitching a water softener. His plan will be to talk and talk, to tire you out, until you're ready to sign. Be impolite and ask right out:

"Hey buddy, why is it I can get the same thing at Sears for only three hundred?"

This will break up the rhythm of his discourse, and he may try to answer you. Whether he does, or whether he tries to brush the question aside and continue with his sales talk, ask the same question again after about two minutes.

You can throw in some extraneous and misleading comments, even if they're total lies, to break him up. It may be hard to get used to the idea of becoming a ruthless liar, but remember that a salesman is often exactly that. A comment such as:

"My aunt in Oshkosh bought one of those and it blew up the first day," will be a sure stopper. The salesman, if he's sharp, will reply:

"It can't be our brand. We don't sell them as far west as Oshkosh." You know that's a lie, so you throw in a bigger lie:

"Oh yes, it was your brand. It blew up, the fire department had to come, and my aunt sent me the newspaper clipping and it said right in the clipping, 'Your Brand' of water softener."

Get the idea? This sort of repartee can go on for awhile until one or both of you tires of it, and either he leaves voluntarily or at your insistence.

After the salesman leaves, you realize he never should have gotten in the door, and perhaps never should have arrived at your door. Irritated, you resolve that the next time....

The next day, the phone rings: "Hello, Mr. Smith, this is the Acme Donut Hole Company. We'd like to give you a free gift and demonstrate our new donut hole maker. What would be a good time?"

Think. Think hard.

"Come about seven." You know nobody'll be home then.

"Seven it is. See you at 301 West Street." That's just fine. You moved to East Street last month, but why tell them that? If you didn't move, tell them you did. It's always possible they won't take the hint, will call you back and ask where you live, but if you have a common name such as "Smith" you can run your finger down the page and pick out another one.

Turning to how to slip out of a deal if you feel it will turn sour, you can once more hide behind your "lawyer." Even if the deal is a straightforward one, such as buying a car, if the salesman asks you for a deposit, you can avoid writing him a check by telling him you have insufficient funds. He'll immediately come back with the suggestion you write a post-dated check, which is your cue to say:

"Oh, no, my lawyer told me never to write a post-dated check. He says I can be in double trouble if it bounces."

This doesn't have anything to do with anything, but it will stop a salesman cold. Your manner will help, too, if you just shake your head and repeat that your lawyer said "No" and that is that. No matter how hard he tries to pressure you, pretending you can't quite understand his explanations will frustrate him.

This is a good point to discuss an important aspect of the battle of wills between the salesman/con man and the client/victim. The motives may be honest or crooked, but the dynamics are the same. The salesman will use pressure, lies, and other deceptive tactics. Your defenses are more lies, temporizing, and a stubborn refusal. The salesman will perhaps even act boorish, try to make you look foolish, and embarrass you if you don't sign on the dotted line. If you cave in, you'll feel more foolish some days later. Use the time he's talking to think of an excuse not to sign. The lawyer story always works. Use it.

Safeguarding yourself against health frauds means more than just avoiding the snake-oil merchants/faith healers. Be careful with “real” doctors, too. Perhaps the best guide is the recommendation of a friend whose judgement you trust, when looking for a doctor.

Always get a second opinion whenever a doctor suggests either surgery or some radical treatment, such as radiation. If your life is on the line, a third opinion isn't too much. Placing yourself unhesitatingly in the hands of a knife-happy surgeon can be hazardous to your health.

Playing the market, unless you know a lot about it and do it for a hobby, can be hazardous to your wallet. If you get a tip on a stock, or an “investment,” check it out with your lawyer, for real, before spending any money. If you're contacted by a boiler-room operation, use the same tactics as with other types of salespeople.

One exception is if a boiler room gets the wrong number. If they think you're Mister Jones, don't spoil the illusion. By all means order by phone, if they let you, and go along with anything they say.

If you're reasonably well off, and someone, working through a friend or an acquaintance, offers you a chance to get in on the ground floor of an investment in something new, take an extra step to protect yourself. Physically visit the premises, if they are within reach. If not, don't invest. You may get a nasty surprise, finding that a factory which is supposedly producing three hundred donut hole machines a day is shut up tightly.

Most passive and active defense is based on knowledge and common sense. The object is to protect yourself and your wallet from harm. Mostly, the means is to avoid getting “conned.” It follows the old principle that an ounce of prevention is worth a pound of cure.

THE PRINCIPLES OF COUNTER—ATTACK

As we've seen, sometimes passive and active defense are not enough, neither to protect us from being victimized nor to give us the satisfaction of retribution. There will be times when nothing less than a very aggressive measure will do.

Some people get very physical when they are angry. This is a release for emotion, but unfortunately it is also a felony to attack physically. If the attack is in front of witnesses, or if the other party chooses to prosecute, the fraud victim who lets himself be carried away by emotion will be in worse trouble than the con man because, as we've seen, fraud is hard to prosecute. In any event, the police will take a stand against anyone who takes the law into his own hands and beats up his exploiter. Their position is, under the law, that the proper response is to report the fraud to the authorities and let them handle it. A fraud does not constitute justification for a physical attack, under the law regarding self-defense, and the person who decides upon a physical attack has to face the prospect of criminal prosecution if he's seen and recognized.

An intelligent counter-attack consists of evaluating the situation and assigning priorities. The first step is to keep a low profile. In the sense of preparing a counter-attack, keeping a low profile means more than the defensive low profile. To keep the con artist off his guard, it's important that he not know that you, his victim, suspect anything. Setting him up while he thinks he's setting you up is simply good strategy.

The next principle is to gather the necessary information about the swindler, whom we'll call the "target" from now on. What information do you need? That depends on how you plan to strike back, and the amount of time and trouble you're willing to devote to the subject. At the least, you need the basic information to support your tactics. If, for example, you plan to strike back at him through the mail, all you need is his address for the basic methods.

With regards to gathering information in preparation for a counter-strike, it's important to consider the choice of target. Unfortunately, many swindlers are very slippery, and have left the scene before any of their victims become aware they've been had. If this happens to you, you'll feel very frustrated indeed, as your chances of counter-attack will have been foreclosed before you can start.

There is a possible solution to this problem. Any basic text in psychology explains the psychological mechanism known as "displacement," in which a person takes out his anger and frustration on another person or object, not the one who caused his anger. A person who's experienced a hard day at work because of the interpersonal conflict may come home and take it out on the family, for example. This "displacement" causes more problems in its wake, and is not a practical solution to such problems, when the object of the "displacement" *is an innocent person*.

If the target is another guilty one, the situation is totally different. In practical terms, if the con man who victimized you has already fled, you can attack another one. There is no shortage of fraud artists, and transferring your anger from one to another who's more available will do two things:

1. It will give you a psychologically healthy release for your anger and frustration.
2. By choosing another fraud artist, you'll be performing a useful public service. If you impede or break up his operation, you'll be saving other potential victims from going through the harrowing experience that you suffered.

This is one of the few instances in which a psychological defense mechanism, normally a compromise with reality, can offer the best solution to a problem, both in the inner world of feelings and in the outer world of reality. There is also a tactical advantage: By choosing another target, you have the option of being completely unknown to him, and therefore immune to any action he might want to take.

Another principle to follow is to plan carefully. Don't go off half-cocked, as hasty action, unless dictated by time pressure, is usually not the best. In some instances, it might be better to let your target go, and leave town unscathed, rather than carry out a premature attack that probably will not work very well. You can always select another swindler.

Finally, use the multiplier effect for maximum leverage. The multiplier effect means making others do the bulk of the work for you. You set off the spark, but the fire spreads on its own. In practical terms, it means causing your target more expense and trouble than you spent arranging it. We'll see how later.

COUNTER—ATTACKING THROUGH THE MAILS

As many fraud operations use the mails, it's proper to use their own weapons against them. A good start is the postage-paid cards and envelopes. We've already seen in the section on active defense that sending them back will cause the target expense, but there is one step beyond that will multiply his expense.

Anyone with a business reply permit is obligated to pay this postage, no matter what. This means that, if you want to take a little time and trouble, you can wrap a brick in paper, attach a business reply card or envelope, mail it, and force him to pay whatever the cost is. If you want to be even nastier, fill a box with sand or dirt, seal it and attach the card, and think of the satisfaction in making him pay twenty or more dollars postage to receive a box of dirt.

Another way to use the mails against a fraud artist is to place an obviously fraudulent ad in his name in a publication. This will work only if he's going to be at the same mailing address long enough for the authorities to take notice. Here's how it works, in detail:

Your target is the "XYZ Company," which has run a successful scam for which they haven't been prosecuted because of a loophole in the law. Place an ad in a publication with the "XYZ" name and mailing address on it. You don't need to know their street address, if they're using a mail drop or a post office box. The authorities will find it in short order. The ad should read something like this:

"Guaranteed Cancer Cure — send ten dollars for information."

Or: "Become a member of the FBI — Diploma and badge guaranteed."

Many publications take the position that they'll print any ad as long as they get paid for it. It's usually possible to find one that will accept the ad. If you know the company's street address, you may be able to phone the ad in to the local newspaper, asking the newspaper to bill the company. It will usually cost less than ten dollars to place a classified ad.

If you've lodged a complaint against a swindler, but have seen no action because of a loophole, you can place an ad in his name to close the loophole. For example, if you answer an ad for a baldness cure, and the substance you get doesn't work, the police might tell you that the ad did not specifically guarantee that it would work for a particular individual, or some such nonsense. This indicates your line of approach. Place an ad, in the name of the company, that promises:

"Guaranteed to work on anyone."

Or: "Triple your money back guarantee."

This will not only close the loophole but give them a serious problem to boot. It may not even be necessary for you to pay for the ad. If the company's ad runs regularly in a certain publication, it's possible to phone the publication and claim to be a representative of the company, and order a change in the ad. You can instruct them to add the appropriate wording, and let them do the rest. This is a perfect example of the multiplier effect.

In plain language, what you've just done is to "frame" your target. By a sophisticated means, you've planted evidence that will facilitate prosecution and cause additional problems with his running the scam. If you want to get really serious about framing him, you can use the mail for it.

With the furor over "controlled substances" in this country, you can send him drugs in the mail. An envelope with a baggie of cocaine, if you have access to illegal drugs, will serve the purpose. An incriminating note, written on a rental typewriter, can accompany the cocaine, to nail the door shut. The note might say:

"Here's the stuff you wanted. Please hurry up and pay me. You still owe me for the last time."

Of course, leave the note unsigned.

There is no assurance that this will result in the con man's going to prison. However, although an unsigned note and an envelope of drugs, found by the police after you tip them off in an anonymous call, may not result in an air-tight case, it will still be an annoyance, and the con man will have a hard time explaining how the material got into his mail. In the same way, if he tries to claim

he did not order the change in the wording of his ad, nobody will believe him, and the odds of a conviction will have suddenly improved.

The ultimate weapon you can use against the swindler who operates his scheme through the mail is to file a false change of address card for him (or against him, if you prefer) with the Post Office. Select an address in another city to cause further confusion. If you want to get his mail utterly lost, divert it to a mail drop in another city, leaving instructions that they are to forward the mail to an address you select. This address will be false, of course.

Diverting his mail may not work for long before he checks it out with the Post Office and discovers the false address change. He'll annul it, of course, but it will still mean he'll have lost a quantity of checks addressed to him

The most important aspect of counter-attacking through the mail is not to get crossed up and use methods that wipe each other out. Sending him heavy business reply mail will be a wasted effort if you use a change of address card on him.

PUTTING THE HEAT ON THE BOILER ROOM

Boiler room operations, using banks of telephones, are most vulnerable at one point — the phones. Put out the phones and they're dead in the water. There are a number of ways of attacking their phones, but first you need to know where they are and what numbers.

Many boiler room salespeople do not normally give you their phone numbers, instead arranging an appointment for one of their sales reps to visit you, or gaining your agreement to buy stock or precious metals options, etc. Therefore, if you get a phone call of the boiler room type, the first priority is to find out the phone number from which the party is calling. A simple way is:

“Hey, that sounds great, but there's somebody at the door. Can I call you right back in a couple of minutes? What's the number there?”

There are only two possible responses. One is agreement, and disclosing the number. The other is to tell you that he or she will call you back in a few minutes.

If you get the second response, all is not lost. When the boiler room operator calls back, listen to the pitch, and write down any pertinent information. If there's a street address given, it may be possible to go there and, using the stalled car trick, obtain the phone number. This might be necessary because fly-by-night operators are not at an address long enough to be listed in a telephone directory.

If you're being invited to a sales office for a “demonstration” or other purpose, by all means go. Stay just long enough to note the phone number or numbers, keeping in mind that there is usually more than one.

A problem may arise if the phone call is from an out of town boiler room with WATS lines. WATS stands for Wide Area Telephone Service, and is a bulk rate offered by the phone company for heavy long-distance users. If the call is from out of town, you may not be able to track down the address and phone

number as easily. However, many public libraries stock out of town directories, which will make your task easier.

Once you've obtained the obnoxious number, the next step is to decide your course of action. Plan carefully, keeping in mind one action may cancel out the effect of another.

The first, and obvious step, is to interrupt their phone service. The directory will give you the business office number for each phone exchange. A call to the business office, representing yourself as the office manager of the "XYZ Company," and telling the service rep the office is closing for a week, will result in the lines being disconnected at your request. It's that simple.

While you're at it, you might call the power company to have the electricity cut off on the same date. Not having a phone readily available to call and find out why the power's off will delay them further.

It's expecting too much to think this will interrupt their operations for more than a day. It's also a trick that you can use only once. To continue the disruption of their "business," you need other means.

Keeping their lines tied up is another way to slow them down. Placing an ad offering a house or car for sale at an irresistible price will keep the phone calls coming in for awhile.

One method that worked and kept a business's lines tied up for three days was a classified ad offering "free green stamps" to the first thousand people who called a certain number.

Note that in all of these methods there was no need for you to call the boiler room yourself with any disruptive calls. The multiplier effect assured that one phone call from you resulted in hours of hassle for them.

Another way to tie up the phone lines is to offer a free keg of a new brand of beer, delivered to the home, to the first thousand people who call a certain number. For some of the more outlandish ideas, the classified advertising department of a newspaper may be reluctant to accept them.

The way around this is to have a quick printer run some flyers for you. As we've seen previously, printers don't question closely

material run for a paying customer, as long as it's not blatantly illegal, libelous, or pornographic. An 8 1/2 x 11" flyer on cheap white paper, printed on one side only, will run you about five dollars a hundred, and quantity price breaks are available.

Two possible wordings for such flyers are as follows:

FREE INTRODUCTORY OFFER!

NEW BEER DISTRIBUTOR MAKING YOU "AN OFFER YOU CAN'T REFUSE." WE'LL GIVE YOU A KEG OF THE BRAND OF BEER OF YOUR CHOICE ABSOLUTELY FREE, JUST TO GET ACQUAINTED!

NOTHING ELSE TO BUY! NO CONTRACTS TO SIGN! NO OBLIGATION OF ANY SORT!

WE'LL DELIVER ANYTIME DAY OR NIGHT, AT YOUR CONVENIENCE. HOLD A NEIGHBORHOOD BEER BUST, AND TELL YOUR FRIENDS!

WE'LL SUPPLY THE KEG, TAPPER, TUB, ICE, AND PLASTIC GLASSES FOR ONE HUNDRED GUESTS.

NOW HERE'S THE CATCH: WE'LL ALSO GIVE YOU A COPY OF OUR PRICE LIST. REMEMBER, THE FIRST KEG IS ABSOLUTELY FREE, BUT WHEN YOU DECIDE TO HAVE ANOTHER PARTY, YOU'LL REMEMBER THE PRICES WE CHARGE AND YOU'LL CALL US FOR SURE!

FOR YOUR FREE INTRODUCTORY KEG OF BEER, CALL: 123-4567

BOTTLE CAP COLLECTOR NEEDS BOTTLE CAPS

COLLECTOR WILL PAY FOR BOTTLE CAPS. PRICES RANGE FROM ONE DOLLAR EACH FOR COMMON ONES UP TO TWENTY DOLLARS FOR HARD TO FIND BOTTLE CAPS.

CALL 123-4567 TO FIND OUT WHAT YOUR BOTTLE CAPS ARE WORTH.

It won't be necessary for you to spend hours in parking lots placing them on windshields. Leave a short stack of them in every store in a shopping complex, and enough people will pick them up to make the effort worthwhile.

CRAMPING HIS STYLE

This category involves carrying out or provoking actions that will physically interfere with your target's operations. Not all fraud artists are vulnerable to this, but those who are will suffer.

This simple action you can take will work only if the target has a fenced-in yard or parking lot. A water-softener peddler usually needs a parking lot for the trucks used for installation. If the gate is closed by a chain and padlock, putting an extra padlock on the chain one dark night will cause some consternation the next morning. A good padlock will cost upwards of five dollars, which might seem too much money for just a few hours' inconvenience. A tube of cyanoacrylate glue (Krazy Glue) squirted into the lock will seal it shut, making it unnecessary for you to buy another lock to block access.

If you have the target's address, as you need to for the lock trick, there are other choices open to you. One is to place a classified ad that will bring people to his office by the scores or by the hundreds. Free green stamps is one possibility.

Another gimmick that will bring people flocking to his door is to have a quick printer turn out coupons worded as follows:

LUCKY FINDER PROGRAM

**THE PERSON WHO FINDS THIS COUPON WILL
RECIEVE TEN DOLLARS UPON BRINGING IT TO 123
WEST 45TH STREET. PRESENT THIS COUPON AND GET
YOUR TEN DOLLARS.**

NOTHING TO SIGN!

NOTHING TO BUY!

Coupons holding that wording will fit three to a page, with room left over for the company name and address at the bottom. When ordering such printing, do not include the company's phone number if the object is to bring people to the office. Some might phone to confirm the offer is still running.

Another flyer to attract crowds can read like this:

ATTENTION RECYCLERS!

THE ABC COMPANY IS JOINING THE COMMUNITY IN AN EFFORT TO CLEAN UP THE ENVIRONMENT BY RECYCLING CANS, BOTTLES, AND MORE! BRING YOUR RECYCLABLES TO THE ADDRESS AT THE BOTTOM AND RECEIVE CASH FOR THEM!

PRICES ARE AS FOLLOWS:

CANS	\$1.00 each
BOTTLES	\$1.50 each
TIRES	\$5.00 each
NEWSPAPERS	\$1.00/pound

FOR PROMPT PAYMENT, DELIVER MATERIAL BETWEEN NINE AND FIVE WEEKDAYS. IF DELIVERED AT OTHER TIMES, LEAVE THE ARTICLES IN THE YARD, FILL OUT THE COUPON AT THE BOTTOM OF THIS PAGE WITH YOUR NAME, ADDRESS, AND THE AMOUNT YOU BROUGHT, AND WE'LL SEND YOU A CHECK THE NEXT MORNING!

NAME

ADDRESS

NUMBER OF CANS:

NUMBER OF BOTTLES:

NUMBER OF TIRES:

NEWSPAPERS, POUNDS

TOTAL AMOUNT \$

Something that will work well against an unethical used-car dealer is a flier advertising a beer bust:

COME ONE, COME ALL!

TENTH ANNIVERSARY BEER BUST AT MODEL MOTORS,

123 WEST FOURTH STREET.

MIDDLEVILLE, USA.

STARTS AT TEN A.M. AND CONTINUES UNTIL DARK!
ALL THE BEER YOU CAN DRINK! FREE BUFFET-
STYLE FOOD!

STEAK AND RIBS ON THE GRILL! CORN COBS AND
COWBOY BEANS!

COME AND CELEBRATE WITH US! EACH PERSON
ATTENDING WILL QUALIFY FOR THE DRAWING FOR A
NEW CADILLAC LIMO BEING GIVEN AWAY IN
CELEBRATION OF OUR TENTH ANNIVERSARY!

NOTHING TO BUY! NOTHING TO SIGN!

DOOR PRIZES OF FREE COLOR TVS GIVEN AWAY
EVERY HOUR!

BE THERE!

This has to work with a flyer, rather than an advertisement,
because no newspaper is likely to accept anything as outlandish as
that, but a quick printer will.

It helps to tailor the flyer to the sort of target you're attacking. A
water-softener pusher would more logically be giving away water
softeners, not Cadillacs. A pyramid sales office would give away
almost anything, but the door prizes would be cases of their
merchandise. Plan carefully, and the effect will be devastating!

Two "quickies" that will add to the swindler's troubles start with
classified ads you place in his name in the local paper. One reads
like this:

FREE HOROSCOPE

Your future foretold.

No fee, no obligation.

Call 123-4567

HOROSCOPES UNLIMITED

The other one reads:

HIGH-PAYING JOBS, NO EXPERIENCE NEEDED

234-5678

ABC EMPLOYMENT

Both of these will result in phone calls. Note the company names are different. There's a reason for this. When you call in the ads, it might seem suspicious if the same company offered both horoscopes and jobs. The mailing address is the same, but the name is different.

A variation is to give the address in the ad. Employment ads are more likely to bring in walk-in traffic, making them the better choice.

INSIDE WORK

In some instances, you'll have access to the fraud artist's premises. The scam might be a pyramid sales scheme, or other type which makes use of an "office" or "warehouse." As one of the "customers," you may be able to walk in and stay, at least long enough to counter-attack effectively.

It might seem superficially attractive to have "the run of the place," but it isn't necessarily true. Part of your purpose is to strike without detection, and becoming too well known may expose your suspicion. It's best to blend in with the crowd, and do your work casually, without attracting unusual attention.

Exactly what you can do depends on how much access you have to the premises. Some measures you can take require very little, only getting in the front door. We'll consider these first:

If the "business" has a waiting room, lobby, or other area open to the public, and if there are seats and tables with magazines, you can invest a few dollars and cause the fraud artist some embarrassment. Buy some pornographic magazines. They need not be new. Some second-hand, well-thumbed ones will serve the purpose. The sicker they seem, the better. Don't waste your money on those of the *Playboy* and *Penthouse* genre. Buy the ones devoted to sadomasochistic practices, with photos of nude women in chains and the like. Homosexual and lesbian material is equally good. Type up labels with the company name on them, and affix them to the magazines. If you know the name of a specific person, use that. Then go about planting them.

Even if you're a total stranger, gaining access to the lobby is usually easy to accomplish without arousing suspicion. Walk in, with several magazines in your hand, and sit down. Place them on the table, pick up another one, and start to read. The receptionist will notice you soon, at which point you ask for a non-existent person. The discussion ends with your admitting you got the wrong address, and you leave.

If you know someone at the "office," simply bring the doctored magazines with you when you come for an appointment and drop them off at a convenient moment in an appropriate spot.

If you're a total stranger, and have no business there, you still may be able to gain limited access by asking to use the rest room. This will usually cause no difficulty at all if you're well-dressed, well-spoken, and look "respectable." Carrying an attache case will help, in more ways than one.

The attache case contains several plastic bags full of quick-setting cement or plaster, which you pour into the toilet and sink drains. Once the cement sets, it will require a plumber to remove. For best results, the premises should be small, for if there's more than one toilet, the inconvenience will not be as great. Of course, if you can manage to block every sink and toilet in the place, so much the better.

If you have more than just casual access to the premises, there are other choices open to you. One simple one is to smuggle in a gallon can of gasoline, if the local fire regulations have strict prohibitions regarding storage of gasoline indoors. Once you "plant" the can, in a broom closet or storage area, a discreet phone call to the fire marshal's office will start the ball rolling.

The story you tell the fire marshal might go like this:

"I work at the XYZ Company, but I don't want to give my name. The boss keeps a gallon of gasoline next to the furnace, and I'm afraid it might blow up one of these days. I told him I didn't think it was a good idea, but he told me to shut up and mind my own business. Can you do anything about this? I'm afraid of losing my job."

Another counter-measure you can take, depending on exactly how much access you have to the premises, is to stink them out. The first step is to buy chicken parts at the supermarket. They should be uncooked, and frozen. If they come from the fresh market case, pop them into your freezer for a couple of days, to freeze them solid. Keep the parts individually wrapped in waxed paper.

Chicken, when spoiled, has one of the most offensive odors of all meat. Hiding pieces of chicken in an office or shop will make the place unliveable when the meat starts to putrify. That's why it's a good idea to start with frozen pieces of fresh meat, as there will

be no odor when you smuggle the meat into the place. You'll have a comfortable time cushion to plant it and get away.

Planting it where it won't be easily found is the next problem. Although placing it in the air conditioning and heating ducts is an ideal method, it's not likely that you'll be able to unscrew the registers unobserved. Some good places are:

Behind or underneath the seat cushions on a couch.

In the top folds of the drapes.

Open a drawer all the way, and throw the meat behind it.

Behind or underneath heavy pieces of furniture.

Inside boxes containing other items, such as envelopes.

Behind books on shelves.

Under the carpet in a dark corner, if you can pry it up unobserved.

In the walls, if you can unscrew light switch plates unobserved.

On the topmost shelves in closets.

If there's a clothes closet, inside the pockets. This will work especially well if people leave clothing there for several days. Even if they take their coats and jackets home each night, they don't all check the pockets each time, and might take some of these smelly time-bombs home with them.

Of course, unwrap the meat before placing it. You don't want the waxed paper to protect the furniture from the juices of decomposition.

Another means of sabotage, in which they'll do the dirty work for you, is the fake furniture polish can. Removing the label from a can of furniture polish and putting it on a can of spray paint or stain remover will destroy the finish when sprayed on a piece of furniture. If finding furniture polish with a removable label is impossible, have your own printed.

You'll find, with a little imagination, there are many possibilities for retaliation against a swindler if you have access to where he lives or works. The risks are small, the effects great.

DIRECT ACTION

Direct action methods are quick, and easy to use. Sometimes they're all you can use. If the swindler does not have an office or warehouse, if he's the type who operates out of his briefcase and has no permanent address, but is staying in a hotel or motel, your choice of targets is limited. A few quick and dirty methods may be all you can use in the limited time before he leaves town.

Almost everyone has a car these days, and that's a logical starting point. The car may belong to the swindler, or it may be a rental, but working on the car will at least deny him the use of his wheels. If he owns it, so much the better.

A rule of thumb is, if it's a current model car, it may be a rental. A car more than two years old is not likely to be a rental car. Some rental agencies use window stickers, distinctive license plate frames, or other means to identify their cars.

One of the simplest means of denying him the use of the car, and probably causing him some repair bills, is to squirt cyanoacrylate glue in his locks. This glue sets in a minute or less, and is very hard to remove. If he normally leaves his car unlocked, a squirt in the ignition lock will prevent him from starting the car. If you have enough time, and enough glue, squirting a film of glue on all his door gaskets will keep him out of his car.

Cyanoacrylate glue is commonly available under various trade names, such as "Krazy Glue." It will glue almost anything to almost anything else. A few other uses to which you can put this glue is to squirt some into the door and window locks of his hotel or motel room. The moments when he's trying to get into his car will give you an opportunity to do this. If he has a permanent address, you can do the locks there.

A very quick and dirty method of attacking his car is to run a point of a can opener down the entire side of his car. A scratch such as this, running through several body panels, is expensive to repair, and is worth doing if it's his personal car. If it's a rental, it won't hold him up for a minute.

His car finish is also vulnerable to spray paint or paint thinner. Either one will ruin his paint job. He won't care if it's a rental car, but in that case, spray the paint on his windows.

Occasionally, it's possible to find some zany bumper stickers, with legends that can cause embarrassment or more serious trouble for the driver of a car that has such a sticker displayed. Slogans such as:

"Follow me if you're gay"

"God is dead"

might cause a serious incident for the driver. More inflammatory slogans, especially those with a racial content, will almost guarantee that sooner or later he'll be rammed "accidentally on purpose" or become involved in an incident.

Some printers specialize in printing bumper stickers in quantities of one or two. They may cost as much as two dollars each, but that's not much at today's prices.

IMPERSONATION

Impersonating the swindler is a very effective technique, especially as you won't have to do it in person. A vast amount of business today is done by telephone, which makes it relatively easy to play this game. Swindlers do it all the time.

With even a little imagination and time, you can do an incredible amount of damage by pretending to be the swindler. Starting with some of the simplest methods, you can work up to some more sophisticated and far-reaching ones.

What you can do by phone, as with everything else, depends on your target's situation and how much you know about him. Not every method will apply to everyone.

If your con man, for example, is staying in a hotel room, as in **running phoney job interviews**, you can call room service in his name and have unwanted meals sent up. You can call the desk to have the hotel rent a car in his name. If he already has a rented car, you can have it sent back, if the hotel has a parking garage in which the client turns over the key to the attendant.

Using the telephone is vital in the "crossfire" technique. This is when you set one person against another, slipping away when the fight starts. Here's how it works:

You call the hotel garage, impersonating the con man, and order the car washed. The reply may be that the hotel does not offer the service, or there will be a slight delay. Find out the name of the person who answers and then call the hotel office to complain about this. Be utterly unreasonable, and use obscene language, especially if the person who answers the phone is female. The point is to be as abusive as possible, which will result in the clerk putting the manager on the line. At this point, you say:

"If I wanted to talk to you, you #\$\$%&*, I'd have asked for you," and hang up.

Immediately call the swindler. Identify yourself as Joe Blow, the garage attendant, and tell him what you think of him, and add if you ever see him, you'll get violent. During this call, be as abusive as possible also.

If the swindler operates out of an office building, or other rented premises, calling the landlord or manager and becoming abusive will start the ball rolling. The chances of success are much greater in this instance, because the swindler's "company" will most likely have several employees. In the case of the hotel manager, he might realize, if the swindler's voice is quite different from yours, that all is not as it seems, but when there are several people on the premises, and if you just identify yourself as "Acme Vacuum Cleaners," the crossfire technique is likely to work.

Impersonating the swindler, or one of his employees, is useful in another way in a "boiler room" operation. You can call potential victims yourself, making the most outrageously fraudulent claims on the phone. If you choose to do this, select your list carefully. Calling attorneys, prosecutors, postal inspectors and police officers, if you have their home numbers, will improve the chances of getting results. So will calling officers of the Chamber of Commerce and Better Business Bureau. The chances of getting their home numbers are much greater, as typically police officers, judges, prosecutors, and the like have unlisted numbers.

If there's a consumer protection group in the area, they will be a very good choice. Tracking down and stimulating official action against consumer ripoffs is their specialty, and they're the ones likely to make the most intense efforts.

You can also use impersonation as a follow-up to having the utilities cut off. After the con man makes the necessary calls to have the electricity and phone service restored, you can call up the business offices of the telephone and utility companies and berate **them for being so stupid as to accept a phoney call. Again, the key is to be extremely abusive. This will work best with the phone company, because there is an FCC regulation regarding obscene language used on the telephone. Normally, the telephone company is very lackadaisical in its attention to this, as anyone who has tried to complain about obscene phone calls knows, but when someone does it to them, they will move. The retaliation will be, if they take it seriously enough, to cut off the phone service permanently.**

This technique can be so effective that it's worth laying out in detail:

"Business office, Mary speaking."

"Hello, I'm calling about that stupid business where you cut off my lines yesterday. How could you be so stupid?"

"I'm sorry, sir, but someone called here, claiming to be from your company, and said you were closing the office for a week. We had no way of knowing it wasn't legitimate."

"What the #\$\$%& is the matter with you people? After the high rates that you #\$\$%& charge me, you can't even keep your heads on straight?" (Note the unreasonable tone, and the ignoring of the business representative's explanation.)

"Sir, you don't need to use language like that. I'm only trying to help you."

"Help me? You can help me by #\$\$%& my **&\$\$%. You and your company can't even #\$\$%& help yourselves."

"If you continue to use language like that, I'll have to report you to my supervisor."

"Go ahead. She's probably a #\$\$%& like you, too. In fact, when I get back to the office, I'll probably call the president of your #\$\$%& company and tell him that, too." (Note the subtle touch here. Telephone company offices with electronic switching equipment have the facilities to determine from what phone a call originates. You take care of the question of why he isn't calling from the number in question very effectively with that last sentence.)

"This is the supervisor. What do you mean, using language like that to Mary?"

"She's heard it before, just like you have, you #\$\$%&. You sound just as #\$\$%& stupid as she does. Are you going to give me the same bullshit excuses she did?"

"I don't know what Mary told you, but your using language like that won't help."

"I don't care what you tell me. Both of you are #\$\$%& stupid and I don't see how you keep your #\$\$%& jobs. If you two #\$\$%& worked for me, you'd be out on the #\$\$%& street."

“If you don’t stop using that abusive language, I’m going to hang up, and disconnect your service.”

“You don’t dare, you \$%&#*.” (Sooner or later, the supervisor will hang up on you. That is when you go into phase two. You call up the manager of the office of the President, and become as abusive to the secretary who answers as you were to the business office people.)

“Those #\$\$%\$#* idiots at the business office were really nasty and stupid, those #\$\$%*&%\$. The dumb #\$\$%*&% threatened to cut off my phone, the #\$\$%&%&*.”

With a few such phone calls, made from a pay phone, you can cause your target such grief that the effort for you will be well worthwhile.

PLANTED EVIDENCE

If you're really serious about hitting back hard at the swindler, you might consider framing him on a drug charge. Doing it by mail is uncertain, but physically planting the evidence will work every time.

Planting evidence is sometimes known as "flaking," a term that refers to the evidence falling on him as a snowflake would. You have several choices available, if you decide to flake him. If you have access at all to his hotel room, office, or other premises, planting an envelope of drugs is easy. It takes only a moment to open a desk drawer and drop it in. Asking to use the toilet gives you the chance to slip it in the medicine chest.

Much depends on your having access to "hard" drugs, and the amount of money you want to spend. The law in some states distinguishes between "users" and "pushers," with the distinction depending on the quantity found. It's worth checking this out before starting.

In some instances, it will be easier to plant it in his car than anywhere else. One bonus of this is that some states have laws stating the car is to be confiscated if drugs are found inside it. Whether the car is a rental or his personal one, this will make waves, as even if it's a rental car, the rental company will sue him for the value of the car, adding to his problems.

Informing the police is the touchy part. The police receive crank calls each day. They also receive spurious "leads" from malicious people. To make the police act, you have to be convincing. At the start, you're handicapped because under no circumstances do you wish to identify yourself.

The first step is to call police headquarters and ask for the narcotics detectives. When one gets on the line, one story that you might use is the following:

"There's a new man in town. He's trying to cut into the action. His car is parked in front of ——— and he has an envelope of smack in his glove compartment."

If the car is locked, you might have to slip it in through a crack in the window, to land on the seat. Another possibility is to put it inside the hubcap, which is one possible hiding place for someone carrying contraband.

The detective might want to know who you are or why you're telling him. Naturally, you won't give your name. You also should be aware that the detective will wonder which of the regular dealers is informing, if he accepts your hypothesis. If he does not recognize the voice, he may not accept your story, which is why you should whisper into the phone to leave this doubt open. He won't be able to say you are one of the regulars, but neither will he be able to say you're not.

It is a psychological quirk that people are more ready to believe a story someone tells against himself. You can take advantage of this by using a story against yourself if the opportunity comes. A couple of possibilities are:

You're a drug addict, and the target sold you impure stuff.

If the detective insists on knowing your motivation, you can tell him outright you're a jealous lover (it's all right to admit being **homosexual for the story — the detective doesn't know who you are) who is informing just to get his betrayer in trouble.**

If you use a convincing manner, and a have little luck, the police will get a search warrant and follow up on your call. This points up one advantage of planting the evidence in a car. The police can, if the car is unlocked or if the stash is in a hubcap, make a discreet search without the bother of a warrant. When they find it, they go back and get a warrant to make it legal.

You can use almost anything as planted evidence. In a state or city which has strict gun laws, planting a firearm will result in an arrest. Stolen property is another good one. Whatever you choose, you must tailor it to the local conditions, and be prepared to improvise.

LONG-RANGE TECHNIQUES

Often, the fraud artist is unapproachable by direct means. He may be literally a fly-by-night, here just long enough to work his scam and gone the next day. If he's using an alias, for all practical purposes he's gone. The police may be able to trace him, but a private citizen may have a much harder time of it. While there are skip-tracing techniques, they cost time and money. Not all of them are as simple as sending an envelope to the target through the mail with a "Return Receipt Requested, Show Address Where Delivered."

The reason for this is the swindler is a pro at doing a disappearing act. Typically, he'll make a hasty exit, leaving no forwarding address. Without time, effort, and the resources of an organization, the victim has little chance of finding him.

There are a few ways in which the victim can try to find his victimizer, without excessive time, cost, and effort. The key is that the swindler conforms to a pattern. He tends to use a successful method again and again.

An example would be a fraud artist who advertises a "vacation" contest in a national magazine.¹ He'll run the ad, wait for a very few weeks to get the responses, mail out the "winning" letters, collect his money, and he'll be gone. If he's used a post office box, one day the box will just continue to fill up, as he'll stop coming to collect the mail. If he uses a letter drop, he'll rent it for only two months, leaving no forwarding address when his rental expires. Tracing him down to the letter drop will usually be futile, as the people who operate letter drops understand they're not to inquire too closely of their clients, and they don't seek information the client may feel is his business alone. They are professionally unhelpful to any seeking information about their clients. As often the fraud artist will pay in cash, there'll be no record of payment that is traceable.

The alert victim can, with a little luck, sometimes discover where the swindler has moved. He may, for example, notice another similar "vacation" ad a few months later in another national

magazine. Of course, the address will be different, as will the "company" name, and the vacation spot and accompanying photographs may not be the same, but the overall scheme will be remarkably similar.

One outstanding similarity may be the wording of the ad. People do have characteristic ways of expressing themselves, and often a distinctive pattern of expression will surface. The victim who feels he's read the ad before may well have. The ad may contain the word "hurry" several times, or the phrase "limited time only."

There's reason for caution, however. Keep in mind that swindlers, who have no qualms about victimizing people through unethical, illegal, and deceptive practices, are not above plagiarism, and one swindler may copy the text of another's ad remorselessly.

Another reason for a fraud artist's being out of reach is those who operate by mail are often in another city, and often this is not an accident, as they want to be out of reach. In fact, they may not even run their rackets in the same state in which they have their headquarters, in order to make a casual investigation difficult for most of their victims. A swindler who is running an investment racket will not welcome casual visitors arriving at the site of his "plant" or "mine" and inspecting the facilities. Out-of-state land swindlers don't want their clients to know the parcels they're buying are under water or on top of a mountain.

Sometimes, the swindle is very modest, and on the borderline of legality, and the fraud artist may stay in place for years, secure in the knowledge the victims are not going to look him up for the small amount of money involved. Examples are the various distributors of vitamins, diet pills, and popular music recordings that advertise on television. Typically, the commercial will ask the viewer to send his check or money order to a local P.O. box, which may well be in Portland or Phoenix, while the home office is in Boston. The customer who feels the quality of the records or tapes are not worth the money, or who feels he or she has been ripped off in the purchase of the pills, will usually take the point of view that it's not worth the hassle for "only" twenty dollars. The psychologically compelling thing is that twenty dollars seems to be

the magic figure right now (late 1984). Just as it is a small enough amount for most people to risk on a purchase sight-unseen, so it is not a large enough amount for most people to disturb themselves in trying for a refund or reporting the transaction to the authorities.

A special block of techniques will enable you, the victim, to reach these remote fraud artists. Most of them are adaptations of more conventional techniques. In one sense, the long-range methods are easier and safer to use than most of the conventional ones, as they work at several thousand miles distance, in some cases.

The simplest, least costly, and safest technique is to re-route the mail through change-of-address cards. That's right, cards, plural, because often the swindlers operate through a P.O. box in your city but have their headquarters elsewhere. You'll see the main address on the package you receive, if you send for their material.

Hitting the local P.O. box first will produce the most results fastest, because that's where the checks are coming in. Mailing a change of address card to the "Postmaster" of the ZIP code at which the box is located will do it. When you do this, you can make an extra preparation, if you want to spend the time and money. Divert the mail to a local mail drop² which you'll have rented for the minimum period, and instruct the operator of the mail drop to send what he receives on to another address. This is a good way to "lose" the mail permanently.

Mailing a change of address card to the postmaster in the city where the "company" has its headquarters will divert the mail from the head office. This might have even more serious effects if the local operator simply sends the mail from his P.O. box to the main office. If, on the other hand, he opens up a local bank account for the deposit of the income from the local P.O. box, he may have another means of transferring the money home.

Long-range retaliation works best if you're willing to spend a small amount of money to have some material printed by a local quick printer. Here is a list of the basics. Pick the ones that suit your situation:

1. Letterhead for the swindler's "company."
2. Letterhead for a fictitious company, totally unrelated to the swindler's outfit.
3. Invoices for the swindler's company.
4. Tickets to a non-existent concert or sporting event.
5. Mailing labels.
6. Envelopes to match the "letterheads."

Each of these has its uses. First, the letterhead for the swindler's company is useful in generating fake mail from him, which can lead him into an indictment, or at least complications with the other companies with which he does business. For example, a letter to the local television station that runs his commercials can cause him complications, if it orders the series of commercials extended beyond the original contract, or cancelled, or shifted to three o'clock in the morning. Another way in which you can cause him problems by a spurious letter to the TV station is to order a change of wording displayed on the screen. A simple change of address will have the same effect as a change of address at the post office.

What do you do if you don't know what his letterhead is like? That's really no problem. Either write the "company" a letter on an innocuous subject to provoke a reply and copy from the letterhead they send you, or make up your own. Businesses often change the design of their letterheads, and anyone doing business with your target will probably not suspect forgery if he gets a totally new letterhead.

Another use for the letterhead is to generate spurious and indictable frauds on behalf of the target. One good possibility is to write a letter, offering tickets to a non-existent concert or other event, enclosing a pair of tickets in each letter, and addressing the envelopes to people chosen at random from a city directory or phone book. It need not be a fancy job, as a plain boilerplate text will do. It might run like this:

ONE TIME OFFER

For the first and only time in this city, ABC Marketing Corporation is offering discount tickets to the forthcoming concert

INVOLUNTARY REPOSSESSION or In the Steal of the Night

By John L. Russell 3

AUTOMOTIVE LOCKSMITHING

- How to bypass and remove locked ignitions on GM, Ford and Chrysler autos in two minutes or less
- How to read tumblers from door locks to make ignition keys with and without a keycutter
- Time saving products
- Exploded lock diagrams
- "Fast" door opening procedures
- How to pick locks
- Repossession tips and much more

Foreword

"Involuntary repossession" is the art of repossessing mortgaged chattel without the debtor's knowledge by stealth. In most states in the United States, repossession of mortgaged chattel by stealth is legal as long as there is no breach of the peace. Therefore, it is legal to repossess vehicles in the middle of the night without breaching the peace. After all, there is nothing more peaceful than a sleeping debtor. Because of the obvious dangers in conducting involuntary repossession it is necessary that the recovery specialist be able to effect involuntary repossession as fast as possible. The involuntary repossession methods and procedures discussed in this book should enable the professional to conduct automotive locksmithing and involuntary repossession in three minutes time or less on most American made autos.

Since the quickest method of performing one's job is the best method from the standpoint of service and profit, it is necessary for professional locksmiths and repossessors alike to know all the methods of performing same. The true professional analyzes his job thoroughly before undertaking it, thus, he is able to determine before he starts the best method to use.

In this book consideration is given to fast methods of automotive locksmithing and repossession. This manual deals with the basic techniques used by professional locksmiths and recovery agents the world over. It should be explained, however, that these methods are not limited. Personal cleverness and genius enable the professional to develop new and quicker techniques. Only standard methods are described here. Locksmiths and recovery specialists with an inventive mind will be able to find other methods of their own and improve their skill in the art. It is my hope that this book will act as a catalyst, motivating you to continue and improve your knowledge in the art of automotive locksmithing.

About the Author



John L. Russell 3 is a partner in the firm of Russell and Russell Investigators, a Tampa, Florida based investigative agency engaged in the business of investigative and recovery services and is a manufacturer and supplier of locksmithing, investigative and recovery products.

Russell began his career as a private investigator in 1969 at the age of nineteen. At twenty one, Russell became the youngest licensed private investigator in the state of Florida. He has an A.S. Degree in Criminology and is a Ni-Dan (second degree blackbelt) in Go-Ju-Ryu Okinawan karate. Russell is considered an expert in the fields of electronic surveillance and eavesdropping, electronic surveillance counter-measures, security analysis, automotive locksmithing, direct mail advertising and executive management. In 1977 at the age of twenty six, Russell became President of the Florida Association of Private Investigators, Inc., the youngest ever to hold that position. His firm is a member of the Florida Association of Private Investigators, the Private Detectives Association of New Jersey, the International Detective and Recovery Association and the Associated Locksmiths of America.

Table of Contents

Chapter I – Basic Locksmithing	5
Pin Tumbler Systems	5
Side Bar Systems	8
Impressioning and Lockpicking	10
Vehicle Entry	16
 Chapter II – Ford and Chrysler	 21
Door Lock Removal	21
Cutting Keys By Reading the Tumblers	25
Locksmithing Techniques for Ford Ignitions	28
Locksmithing Techniques for Chrysler Ignitions	40
 Chapter III – General Motors, American Motors and	
Chrysler Tilt Wheel	48
Cutting Keys by Reading the Tumblers	48
Reading the Tumblers on the GM Door Lock	48
Reading the Tumblers on the American Motors Door Lock	53
Locksmithing Techniques for GM, AMC and	
Chrysler Tilt Wheel Ignitions	53
 Chapter IV – General and Miscellaneous Information	 62
Key Code Information	62
Motorcycles	64

Chapter I

Basic Locksmithing

To fully comprehend the procedures discussed in this book a basic understanding of locksmithing is necessary and the novice should pay close attention to this first chapter.

Generally, there are three basic types of lock systems that are differentiated by their tumbler usage. The three systems I refer to are; the pin tumbler system, wafer tumbler system, and the side bar system. The wafer tumbler system will not be discussed in this book, neither will another type, the warded lock system. Wafer tumblers are like those that are found in a Volkswagen and warded locks are like those that are found in handcuffs, padlocks, and the old home-type door locks that use a skeleton key.

Pin Tumbler Systems

The pin tumbler system is that that is used in Ford and Chrysler automobiles, in both the ignition and trunk lock mechanisms. Chrysler does have an exception in some of its older models, in that it used a wafer tumbler system, in the trunk lock.

The pin tumbler lock is composed of an inner cylinder and an outer cylinder. The inner cylinder is sometimes referred to as the plug, core or cam. Hereafter it will be referred to as the plug. The outer cylinder is sometimes referred to as the shell or just simply the cylinder. The outer cylinder will hereafter be referred to as the shell. A series of two piece tumblers are mounted in the shell of the lock and extend down into the plug. In both Ford and Chrysler cars, there are five tumblers. The bottom pin is called the bottom pin and the top pin is usually referred to as the driver. The tumblers are spring loaded, with the spring resting on top of the driver pin. The springs and pin are held in place by a spring retainer clip. Figure one depicts a lock cylinder without a key. Notice how the bottom pins proceed down into the plug. Figure two depicts a cylinder with a proper key from the front view. When the proper key is inserted, the bottom pin drops into the plug, and the driver pin rests on the plug. Figure three depicts a cylinder with a proper key from the side view. Notice that the proper key has raised or lowered the bottom pins and drivers so that the key can turn the plug within the cylinder. The point at which the driver pin and the lower pins separate is called the shear point. Figures four and five depict improperly cut keys, and their effect upon the pin tumblers.

PIN TUMBLER LOCKS

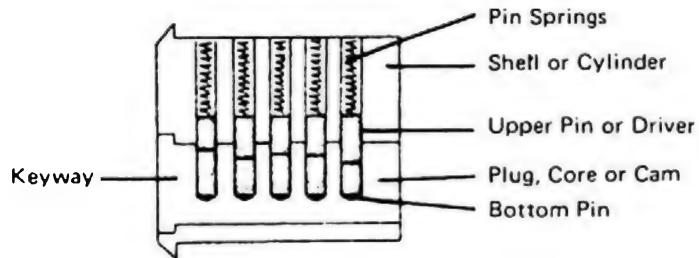


Fig. 1 Cylinder without Key

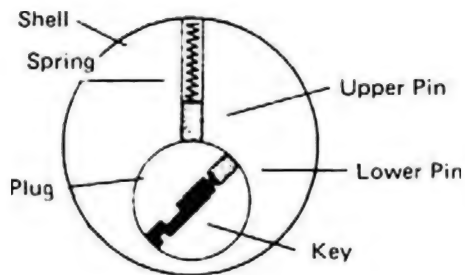


Fig. 2 Cylinder with Proper Key Front View

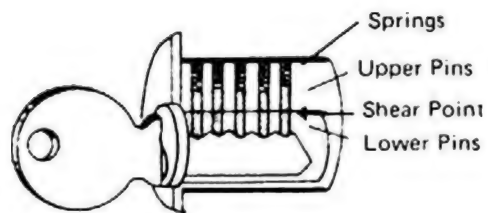


Fig. 3 Cylinder with Proper Key Side View

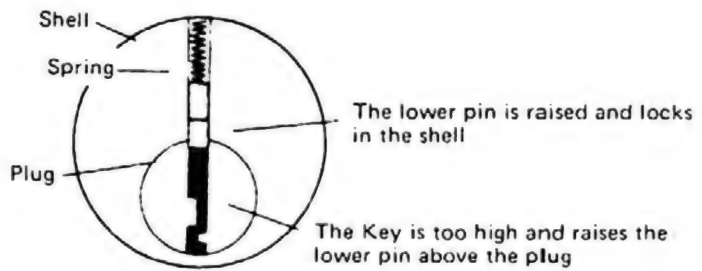


Fig. 4 Cylinder with Improper Key Cuts Too High

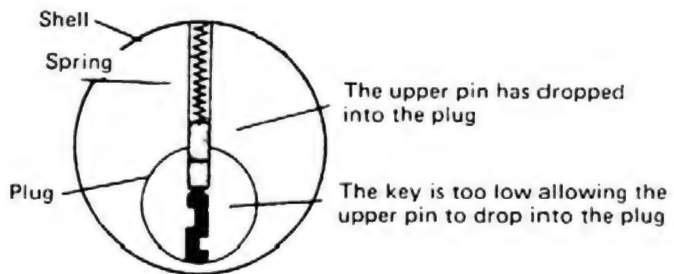


Fig. 5 Cylinder with Improper Key Cuts Too Low

The Side Bar System

The side bar system is that system which is used in General Motors and American Motors products. The basic construction of the lock is similar to all locks in that there is a plug and a shell. Here all the similarities stop. The side bar lock is a modified wafer system consisting of five wafer tumblers or side bar discs in the American Motors system and six wafer tumblers or side bar discs in the General Motors system. These side bar discs are mounted in the plug of the locks, are spring loaded and held in place by a spring retainer. Also mounted in the plug is the side bar. The side bar is spring loaded, and is staked into the plug. When the proper key is fitted into the plug, the side bar discs or wafers are raised, or lowered, so that the side bar slides into the side bar discs and holds them in a straight line. This action allows the plug to turn inside the shell, as the side bar without a proper key extends into a slot in the shell.

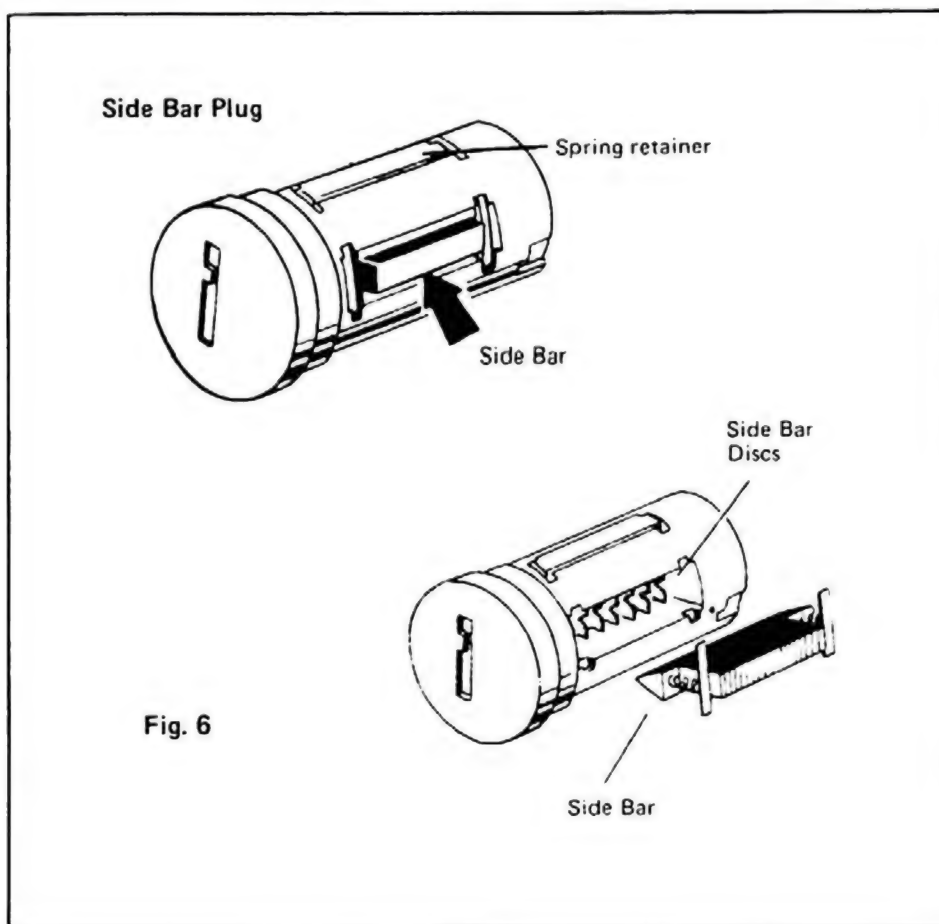


Figure six depicts the side bar plug. Figure seven depicts a side bar lock cylinder with a key too high. Figure eight depicts a side bar lock with a key too low. Figure nine depicts a side bar lock cylinder with a proper key. Notice how the side bar has lined up with the side bar discs, allowing it to clear the slot in the shell, and thus turn the plug.

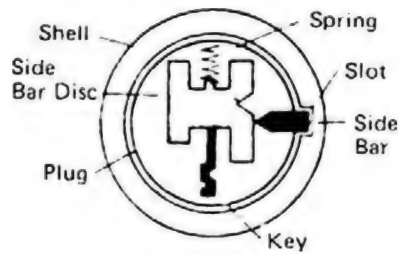


Fig. 7 Side Bar Cylinder with Improper Key - Too High

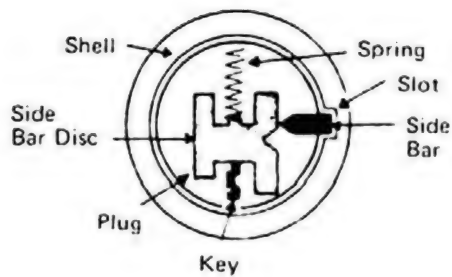


Fig. 8 Side Bar Cylinder with Improper Key - Too Low

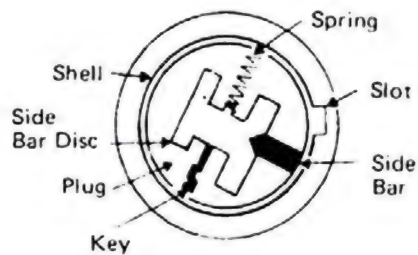


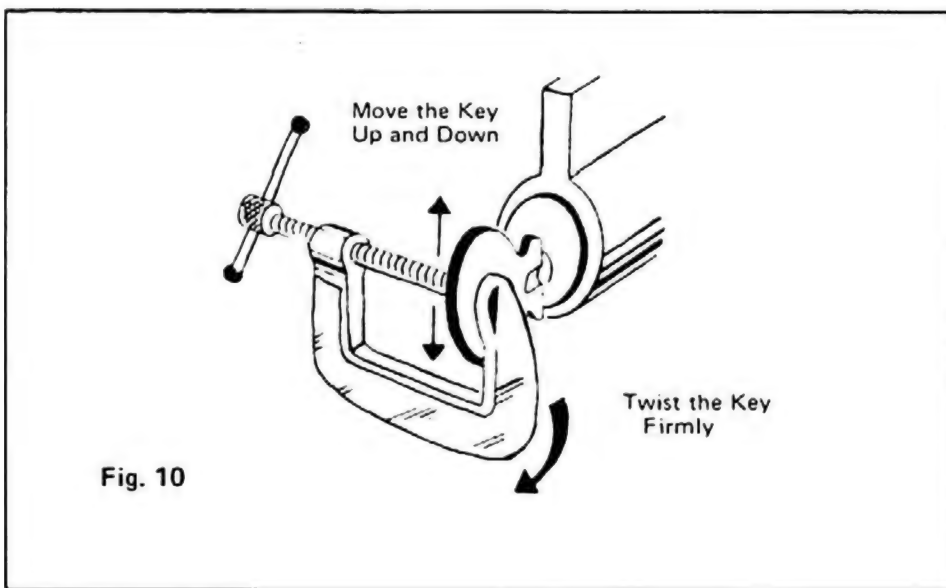
Fig. 9 Side Bar Cylinder - Proper Key

Impressioning and Lockpicking

Of the two systems previously discussed, pin tumbler and side bar, the pin tumbler is the easiest to pick and to impression. General Motor cars, that are of the side bar type, should not be attempted to be impressioned or picked, unless of course you are a lock master. To pick the General Motors side bar lock, a special series of picks are needed, and it takes a considerable amount of time.

One of the most important techniques in locksmithing is the making of cylinder keys by the impression method. If you learn how to do this, you can fit a key to almost any pin tumbler cylinder without having to take it apart or remove it from its location. This system, however, takes long hard practice until it is mastered.

The theory is that a pin tumbler will impress a mark in the blank as you twist it firmly in the plug and at the same time wiggle it up and down. This action will cause marks to appear on the top edge of the blade. When doing this, you should have the head of the blank firmly held in a C-clamp, or vise grips. Figure ten illustrates this technique.



The impression marks illustrated in figure eleven are produced because you bind the pins in the chamber as you twist the key side to side. The rounded points of the bottom pins dig into the top edge of the key blade when you move the blank up and down. As these marks appear the locksmith then files two or three strokes at a time with a round Swiss number four file, being sure to keep his cut smooth as he files only where the marks appear. If they disappear from one location, it means that the pin is no longer binding there and that he must examine the blank carefully to find where the next bind is occurring. Little by little, he files each cut as it marks until he completes the key, figure number twelve. This process takes good eyesight, and patience.

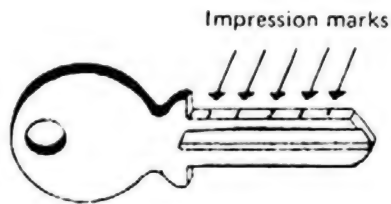


Fig. 11

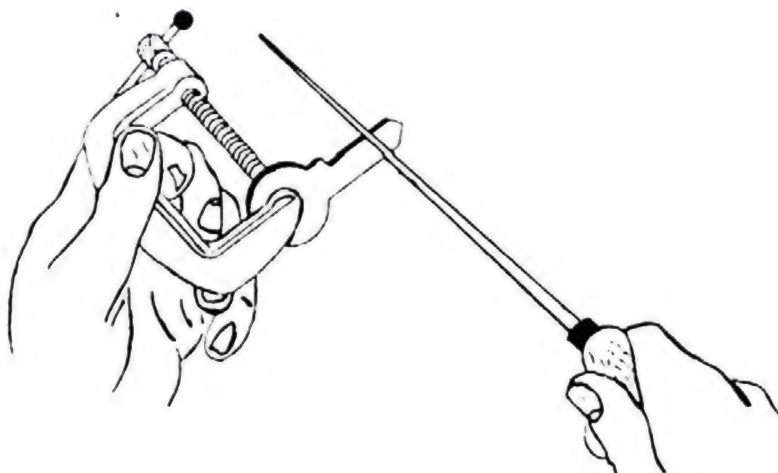
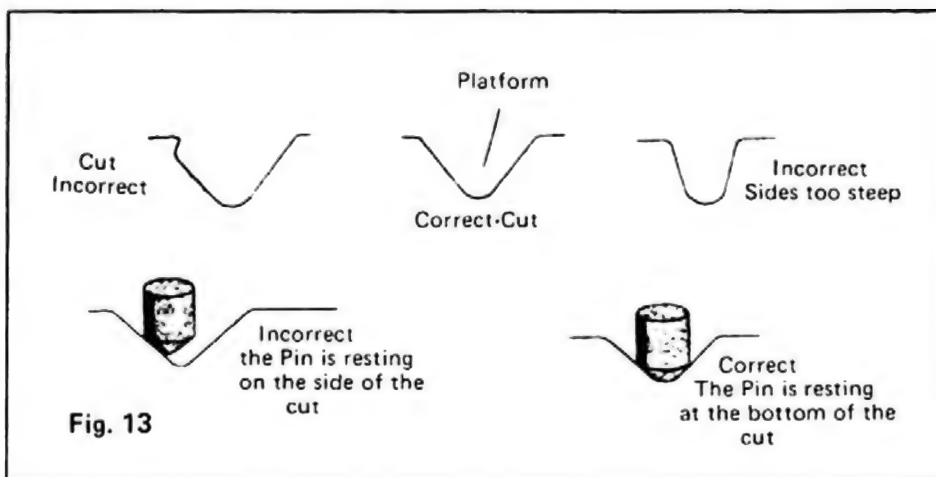


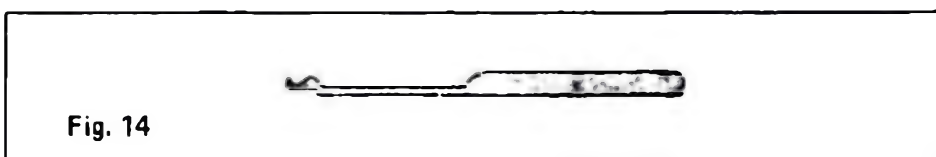
Fig. 12

Do not make your cuts too narrow, and do not leave any "fish hooks" or perpendicular edges on the slopes of your cuts. These may later prevent the insertion or the removal of the key. Widen your cut slightly to leave a small "platform" at the bottom. This is most important, otherwise, your pin may rest on the slope of the notch instead of the bottom. (Figure number thirteen.)

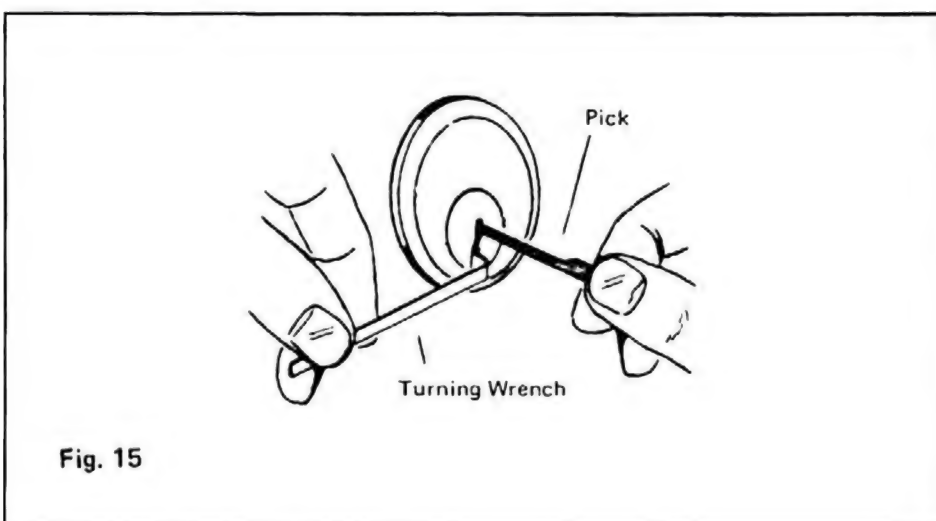


Picking Locks

Nowadays, lock picking is generally confined to pin tumbler or wafer tumbler locks. The idea is to raise the tumblers to the top of the plug so that you can turn it open. Figure number fourteen shows one type of pick that is used.



As you can see, a pick is just a piece of stiff, shaped wire that will enter the keyway of a plug which has just enough room to manipulate the tumblers. A turning wrench or tension tool is inserted into the plug of the lock and turned in the direction that the lock opens. This tension is maintained throughout the lock picking operation. (Figure number fifteen.)



Amateurs try to pick locks by running the pick in and out of the keyway very rapidly while applying turning pressure with the wrench, but this is very haphazard and an unscientific method. In addition, it saws or files the bottoms of the tumbler and often destroys the lock. The true way to pick a lock is to raise one tumbler at a time to the top of the plug and let it "hang" there. When all of the tumblers have been brought into this position, the plug will turn.

The most important factor in picking is the use of the turning wrench. With the proper pressure, you can hold the tumblers that have been brought up to the surface of the plug while still having enough looseness to bring the rest of the pins up. To learn this method take a cylinder and remove the pins and springs from all but two chambers. Learn how to pick these two. Then add a chamber at a time until you have successfully picked the entire cylinder. Remember, this technique takes time and patience.

There are several types of pins, each of which makes the cylinder more secure against picking tools. One type is called "mushroom pins" and is found in Yale cylinders. The other type is "spool pins" and is found in Corbin, Ruswin, and other cylinders. The function of these pins is to hook themselves between the shell and plug and thus prevent lockpicking. (Figures sixteen and seventeen.)

Pin (used as upper pins only)

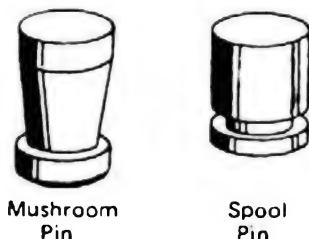


Fig. 16



The Side of the mushroom tumbler is hitting the edge of the cylinder

Fig. 17

Your author has successfully picked both trunk and ignition systems of Ford and Chrysler automobiles. In picking the ignition systems of both these automobiles, there is no need for the tension tool, as pressure can be placed on the chrome knob, or "butterfly" of each.

Other Hints For Lockpicking

1. Use a thin narrow pick, give yourself room to manipulate the pins.
2. Although unprofessional, first try to rake the lock. Worn shells and loose plugs often open amazingly quick this way.
3. Use a reciprocal motion in raking similar to the action of a piston rod in an engine.
4. Hold your pick like a pencil, let your fingers do some of the work as well as your wrist.
5. Steady your hand by resting your small finger against the door.
6. If you use the method of picking one pin at a time use moderately strong wrench pressure.
7. If you use the raking method use a very light pressure.
8. Use a torsion wrench that will not block the keyway so that the pick cannot be manipulated freely.
9. Make sure that the pick can enter above the wrench without raising any of the pins.
10. If the wrench blocks the keyway, try placing it at the top of the keyway.
11. A torsion wrench with a long leg to enter the keyway can be held more firmly and level than one with a short stubby leg.
12. Expertise and technique is developed only by practice.

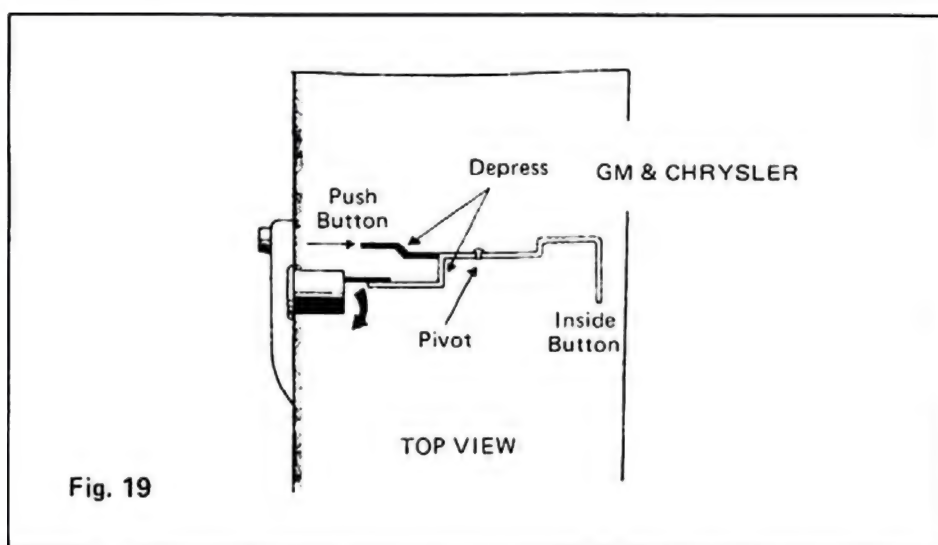
Vehicle Entry

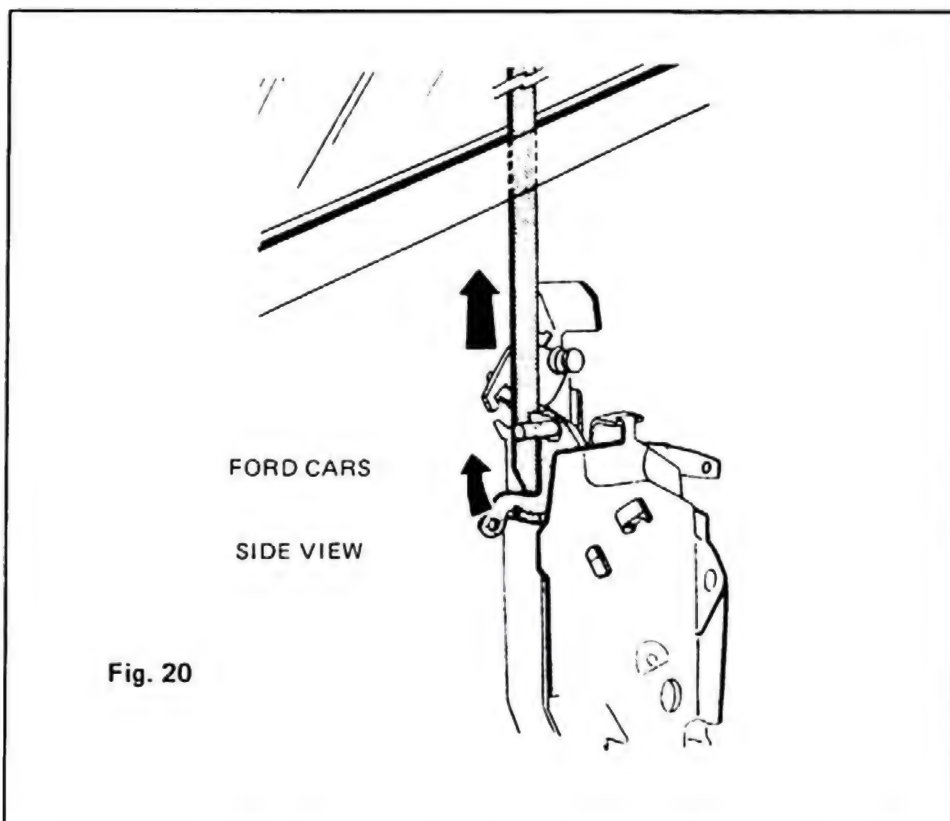
Getting into a vehicle can sometimes present a problem. Most recovery specialists rely on the "old coat hanger", which is perhaps the most commonly used tool. A screw driver can be inserted between the weather stripping and the glass on "coupe" type cars, and a coat hanger easily inserted. The coat hanger is bent, and pulls the knob up and thus unlocks the vehicle. On hard top cars, however, this is sometimes difficult if not impossible. Here, the forcing of a screw driver in between the door jam and the body of the automobile sometimes produces damage to the vehicle. Other times, the knobs have been removed, and all that is there is the treaded wire that the knob was once attached to. In these situations, locksmiths and recovery agents should utilize car opening tools that are available from your locksmith supplier. One of the best tools for hard top cars and those without knobs is the Slim Jim, as depicted in figure number 18. Note that the ends of the tool are



designed differently to actuate the door lock mechanism by pulling up on same with the "A" end or by depressing the mechanism with the "B" end.

Slide the appropriate end between the glass and the weather stripping of the door so that it can catch the door latch mechanism that is directly behind the door lock cylinder. By pushing down on the latch (figure number 19) it is possible to release the locking mechanism on General Motors and Chrysler cars. For Ford cars, the tool should be hooked over the latch (figure number 20) and pulled upwards to release the lock. On some models where the door frame is curved, it is necessary to bend the tool slightly so that the tip reaches the latch properly. Whether to push or pull the locking mechanism as described above differs from model to model and year to year on Ford, Chrysler and General Motors cars.





When using the Slim Jim, always probe around the door lock, where the lock button is located is not significant. Seldom will the lock mechanism be contacted the first time. Movement of the door lock button will indicate that you have properly contacted the door lock mechanism. If contact is not made after probing with the Slim Jim, remove the tool and change the bend in same and try again. Never use force! If force is required, proper contact has not been made. Should the tool become caught in the door, work it from side to side gently until it is free. Some General Motors and Ford products have two layers of weather stripping, one on top of the other. These must be separated and the tool inserted between them. The following are a few hints on which end to use for specific model cars.

American Motors - For late models, use the "A" end of the Slim Jim without a bend in same (use a slight bend on two door hard tops). Insert the tool straight down on the door lock and push to release. For Gremlin and Hornet, insert the tool in front of the door lock slightly and angle down toward the door lock. Push to release.

General Motors - On late models, use the "A" end with a slight to medium bend. Insert the end over the top of the door lock and push to release. On older models and some hard tops use the "B" end with a slight bend. Insert the tool slightly in front of the door lock and pull to release.

Chrysler - For almost all Chrysler vehicles use the "A" end with a slight bend. Insert the tool in front of the door lock and push to release. Chrysler products with electric door locks are serviced the same except that the lock actuator is short and the button moves only slightly. Occasionally try to open the door to see if it is unlocked.

Ford - For most late model Fords, use the "A" end of the tool with a slight bend inserted in front of or directly above the door lock and push to release. Use the "B" end with a slight bend to service economy cars such as the Maverick, Comet and on some older models. Pull to release.

You may find some inconsistency when using the above methods, but for the most part, they are accurate.

You can use the Slim Jim to open windows in the same manner as you would with a coat hanger by slightly customizing it. Drill two holes in either the "A" or the "B" end and attach a piece of piano wire, monofilament fishing line or heavy twine as indicated in figure number 21. To operate this tool, place the noose over the lock button and pull same tight by pulling it toward you. At the same time, pull up on the Slim Jim to actuate the lock button.

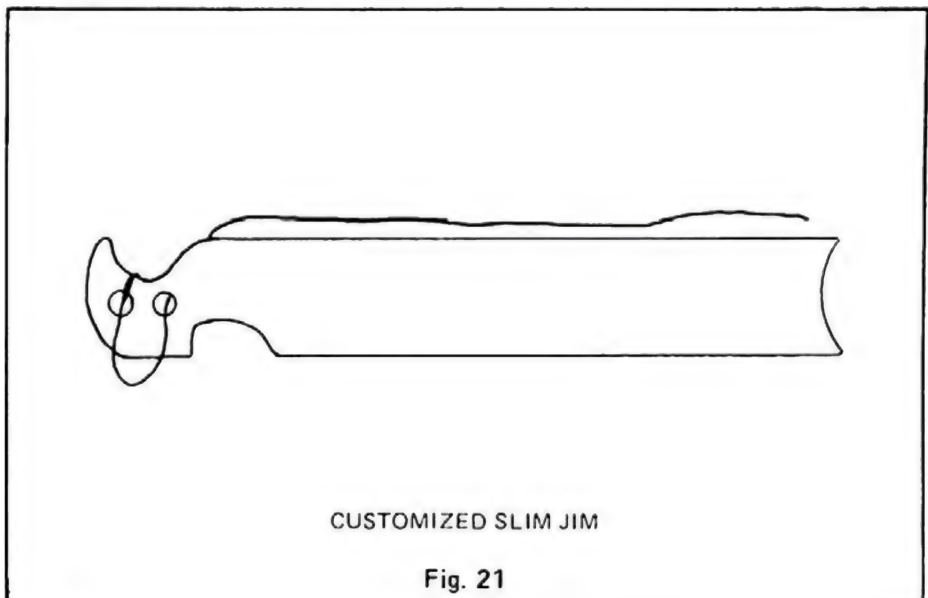
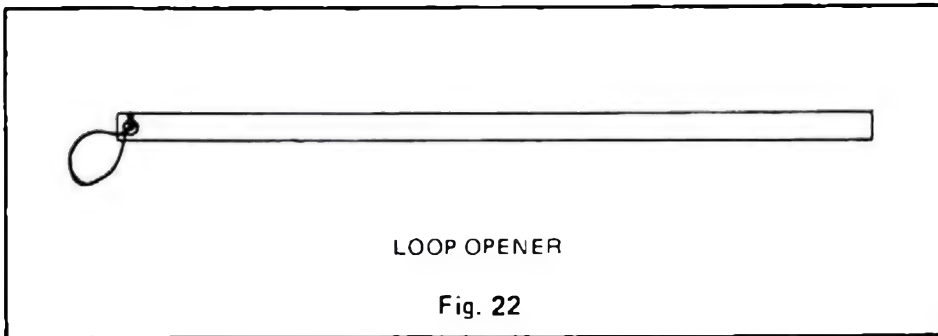
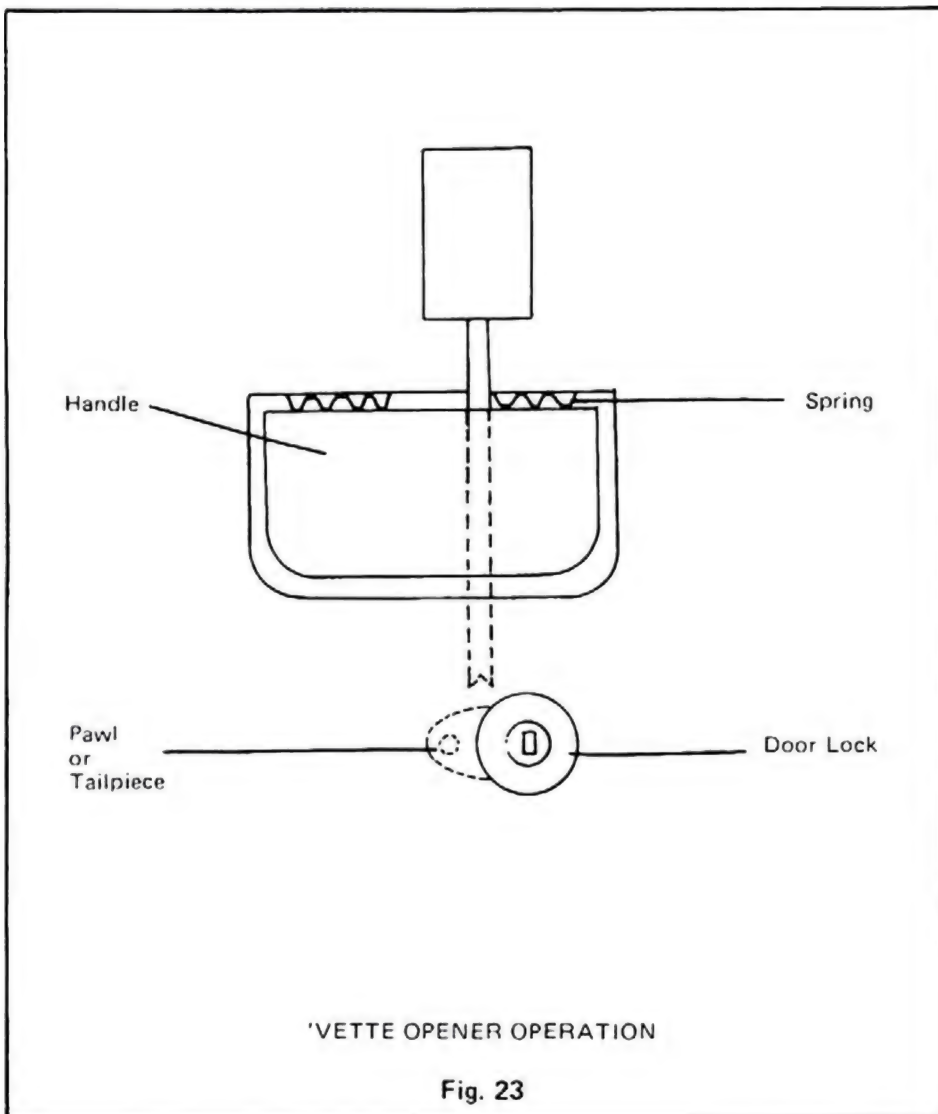


Figure number 22 depicts a handy tool that can be made out of a flexible metal rod. First flatten the end of the rod, and then drill a hole in same. Attach a piece of string, piano wire or monofilament fishing line in the fashion of a loop. To use the tool, place the loop around the lock button and turn the rod until the loop becomes tight. Pull up on the rod to release the button. This tool works especially well when the lock button has been removed and only the threaded wire is exposed. Make sure that the length of the rod you use is long enough to service vehicles having the door lock buttons in the middle of the door.



Opening Corvettes can sometimes be a problem and there are two tools to service this type door lock. The first is similar to the Slim Jim and is used in



the same fashion. This tool is thinner in width than the Slim Jim and is curved like the letter "J". The tool is inserted between the weather stripping above the door lock and comes to rest on the top of the plastic cover over the door lock. By firmly pressing down the lock is released. The second tool, you can make for yourself out of heavy gauge sheet metal or banding material. The tool should be 10" in length, 1/16" thick and 1/4" wide. Use a piece of wooden dowling for a handle. Cut a notch in the "opening end" of the tool so that it will not slip off of the door lock mechanism during operation. To operate this tool, slightly depress the door handle so that you can fit the tool between the hinge at the top of the handle, directly above the door lock. By depressing the tail piece of the door lock, you can release the lock (figure number 23).

There are many types of car opening tools available from your locksmith supplier that are a good investment. Figure number 24 depicts several car opening tools available and their various functions.



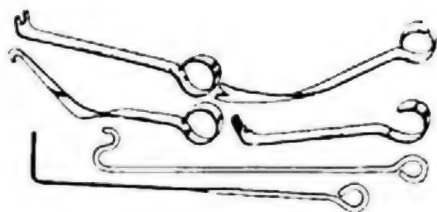
The tool above opens Volkswagen vehicles by inserting it between the weather stripping on the vent window and by pulling the vent window knob open. With the vent window open, the door can be opened by depressing the door handle on the inside of the vehicle.



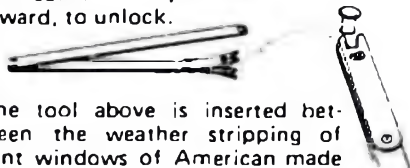
This tool will open most General Motors hardtops, that have the inside locking button located near the end of the door panel. Not for "long-reach" styles as used on late models.



The tool above is inserted between the weather stripping between the front and rear windows on coupes or under the weather stripping of the side vent windows. This three piece section tool is 62" long and actuates the lock button on the opposite door of the vehicle.



Closed prongs, ready to be released and flip button upward, to unlock.



The tool above is inserted between the weather stripping of vent windows of American made autos or rear windows of foreign autos to actuate the door lock button. The notched prongs spring upward to unlock the door.

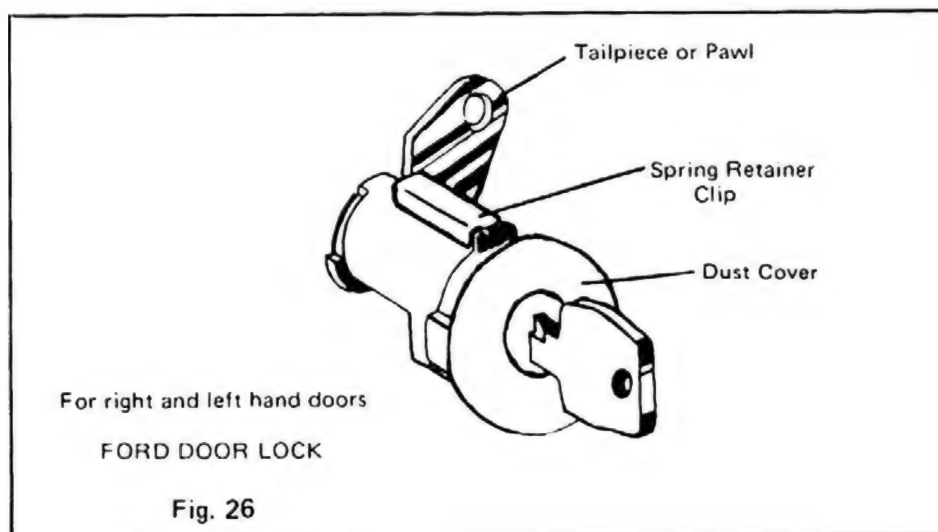
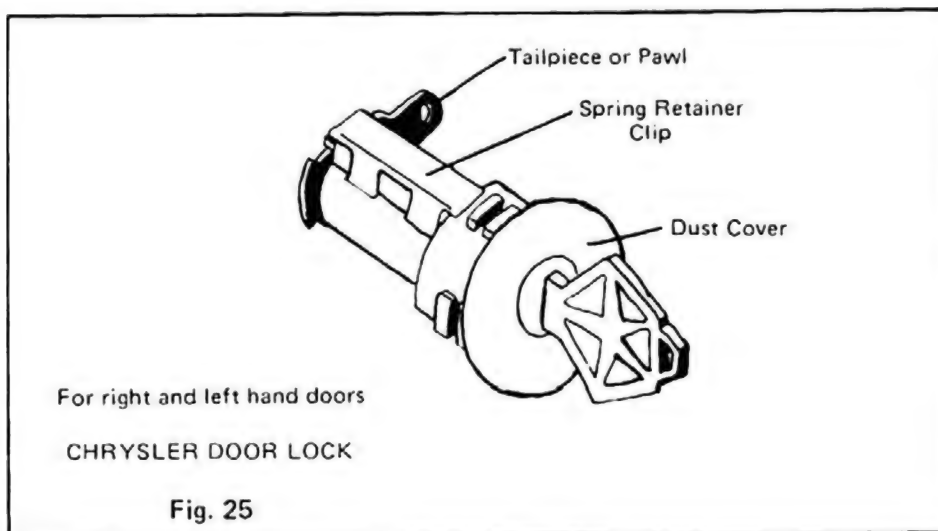
Four of the opening tools above are used to open American made autos with vent windows in the same manner as the VW opener. The other two tools are used to roll the window down or depress the door lock handle on the inside of the car.

Chapter II

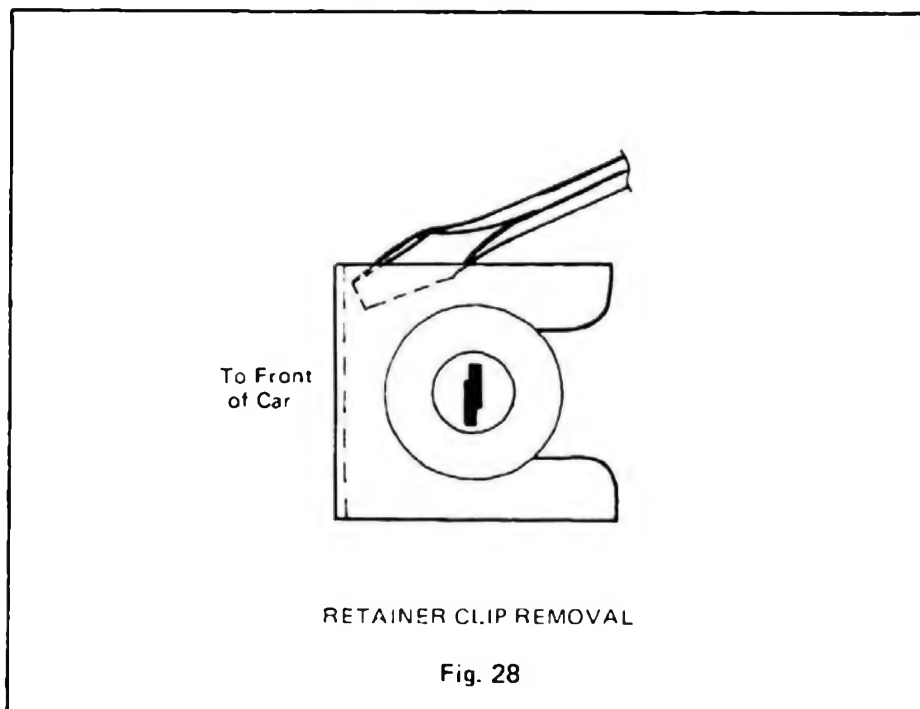
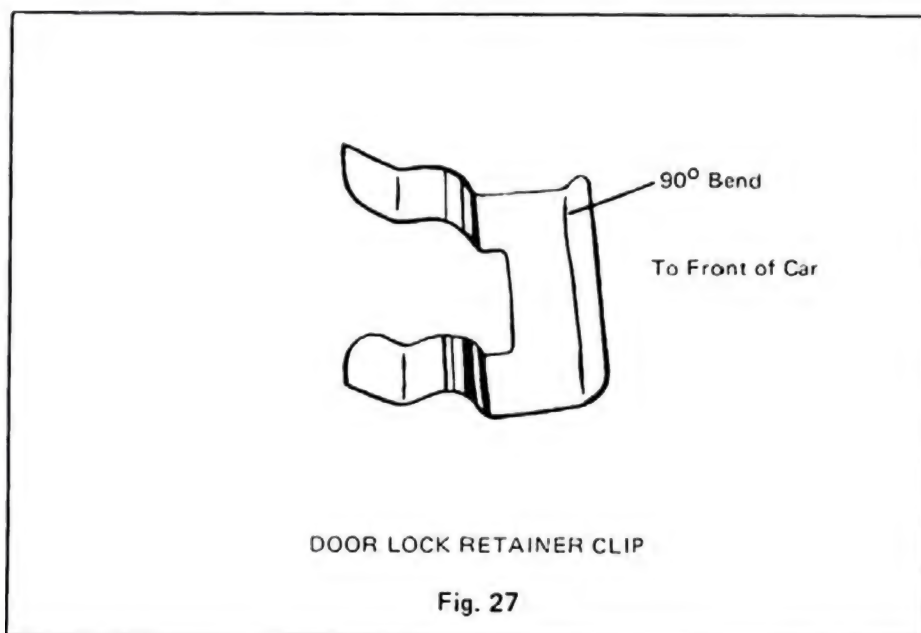
Ford and Chrysler

Door Lock Removal

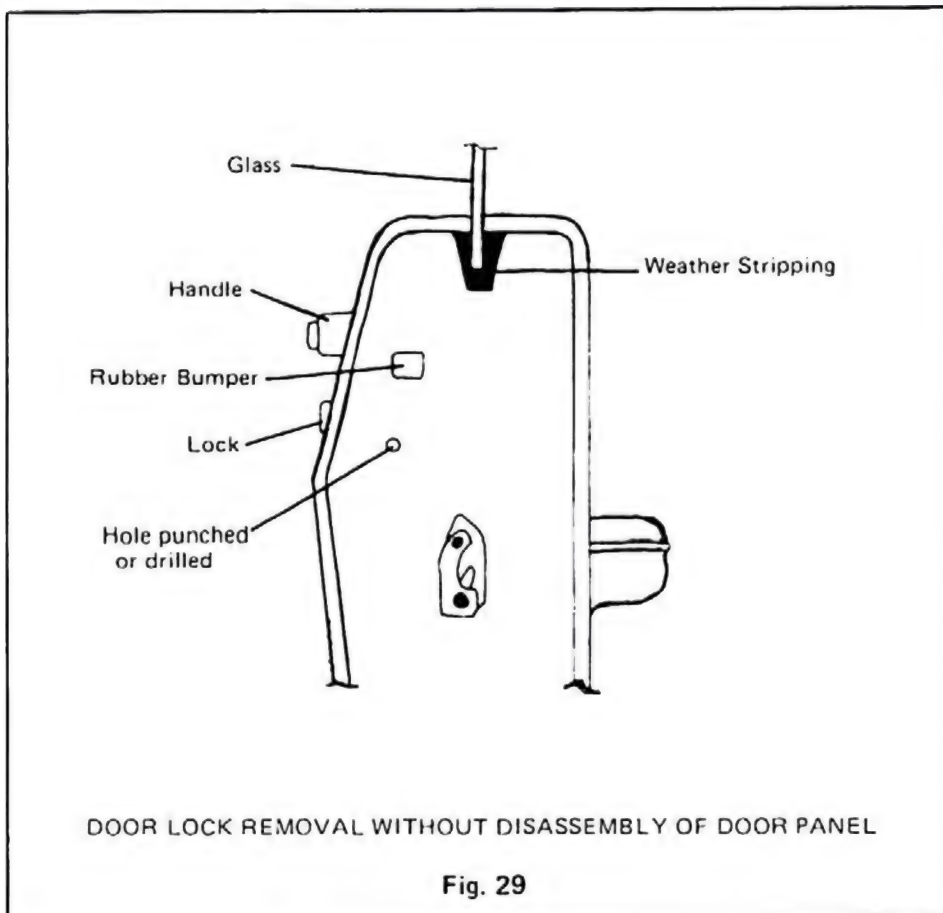
A standard method of automotive locksmithing is removal of the door lock so that a key may be made by reading the tumblers. Figure number 25 is a door lock cylinder for Chrysler products and figure number 26 is the door lock cylinder for Ford products.



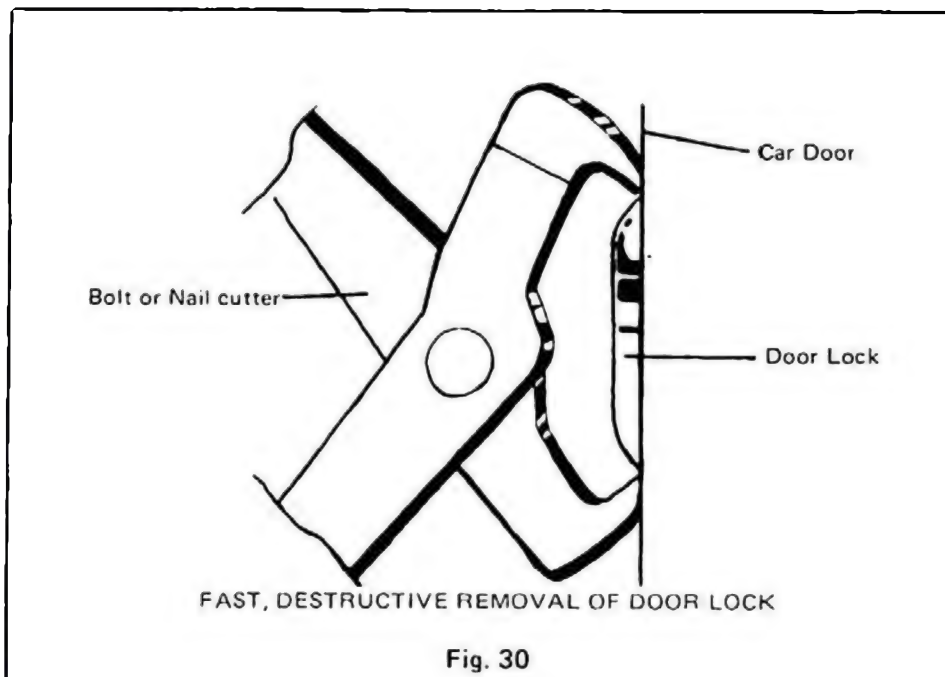
Door lock cylinders in Ford, Chrysler and General Motors cars are retained by a door lock retainer clip (figure number 27). In most cases, the ninety degree bend is toward the front of the car, so the clip can be removed by pushing the clip off with a screw driver (figure number 28).



Take a long screw driver of approximately eighteen inches, and remove the clip by the following methods; place the screw driver through the weather stripping around the glass window on the inside of the door jam and push the clip off, or remove the rubber bumper on the inside on the jam insert your screw driver and push the clip off, or if the particular car has no weather stripping or rubber bumper – take a punch and a five pound hammer and punch a hole inside the door jam – then insert the screw driver and push the clip off. The slight amount of damage that this does to the car is usually not noticable (figure number twenty nine).



A quick method of removing the door lock, that does produce some damage to the vehicle, is by using a pair of bolt or nail cutters. Place the bolt or nail cutters around the outside of the door lock (figure number twenty eight), and by using a prying method and a up and down-side to side motion, pull the door lock out. The up and down-side to side method bends the door lock retainer clip and allows you to remove the cylinder. This method works well on Ford and General Motors cars, but does not work on Chrysler. The Chrysler door lock cylinder is of light pot metal and has a tendency to bend under the pressure of the bolt or nail cutters. By using the bolt or nail cutters, it is possible to remove locks from Ford and General Motors automobiles in less than three seconds. Bolt cutters can be purchased from Sears for about \$6.00.

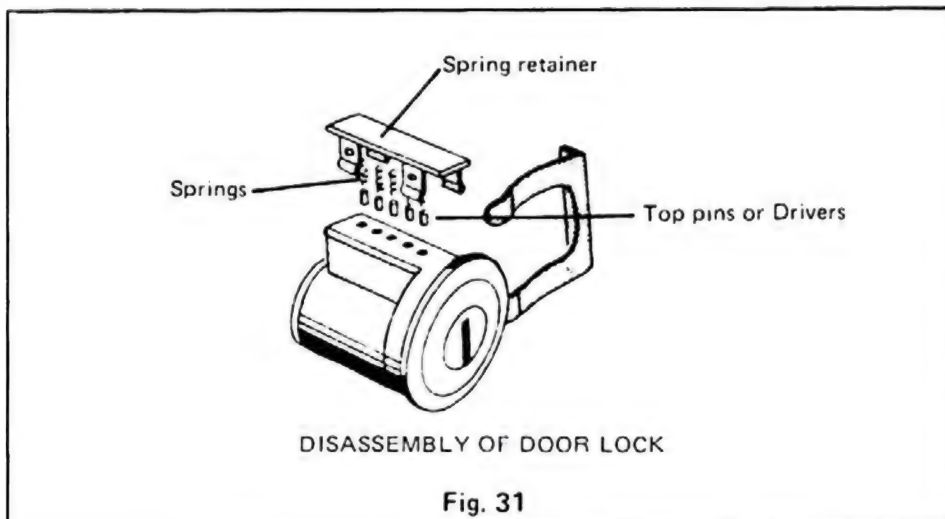


On 1969 General Motors products, the key code to the ignition and door lock is on the door lock. On nine out of ten Ford models, the key codes are on the door lock. Very rarely are the key codes found on the door locks of Chrysler cars, however, your author has found them on the driver's side of the vehicle on 1969 and 1970 models. When you find the key code on the door lock, it is very easy to cross the code and cut the key with a key cutter. If you do not have a key cutter, you should seriously consider getting one.

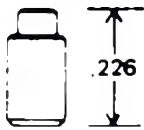
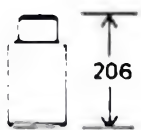

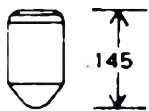
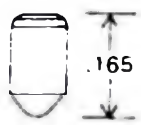
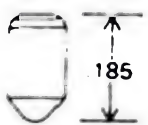


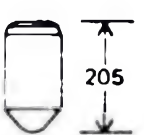
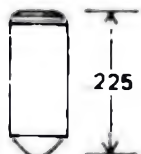


Previously in this section you were advised that the ninety degree bend most often faces the front of the automobile. In some cars, however, this is not always correct. Thunderbirds and Lincolns, often have the door lock clip exposed. In other words, if you open up the door, you will see the clip on the inside of the jam. The door lock cylinder can be removed easily with the use of a screw driver in these cases. On some Chrysler model trucks, the door lock clip faces down. This is true of 1975 Dodge "Power Wagon" trucks. In this case, it is quite easy to roll the window down and push the clip off with a screw driver by putting it between the glass and weather stripping at the top of the door.

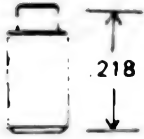
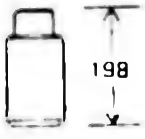







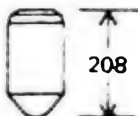
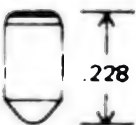




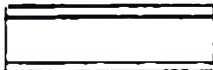

Cutting Keys by Reading Tumblers

To cut a key by removing the tumblers on pin tumbler locks, several methods may be employed.



First remove the spring retainer cap, and the springs. Be careful that you do not lose any of the springs, or turn the cylinder upside down so that the tumblers are lost. Next use a paper clip that is bent at a ninety degree angle or the curved hook pick that is with most pick sets, to remove the bottom and driver pins. Start from the front of the lock at the keyway and work to the back. As you remove each pin set, place them into a small container separately and in order so that you may be able to remember in which order they appeared and replace them if necessary (figure number twenty seven). Next read the cuts of the tumblers by the use of the caliper or micrometer. Figure number twenty eight shows the length of Ford tumblers, and figure number twenty nine shows the length of Chrysler tumblers. After practice, you will be able to determine the length of the tumbler sets by eye. In figure number twenty eight, the bottom tumbler of a number one cut is approximately the same length as the top tumbler (driver) of a number five cut. The top tumbler (driver) of a number one Ford tumbler is approximately the same length as the bottom tumbler of a number five cut. The number three cut bottom pin and driver pin are approximately the same length. In Ford products, there are only five cut depths, while in Chrysler there are six depth cuts. There is little visible difference between Ford and Chrysler pin sets to the naked eye, except the number six cut, and the diameter of Chrysler tumblers is smaller than Ford's.

<p>Top Tumbler No. 1</p> 	<p>Top Tumbler No. 2</p> 	<p>Top Tumbler No. 3</p> 
<p>Bottom Tumbler No. 1</p> 	<p>Bottom Tumbler No. 2</p> 	<p>Bottom Tumbler No. 3</p> 
<p>Top Tumbler No. 4</p> 	<p>Top Tumbler No. 5</p> 	
<p>Bottom Tumbler No. 4</p> 	<p>Bottom Tumbler No. 5</p> 	
<p>Springs</p> 	<p>Retainers</p> 	<p>Fig. 32</p>

<p>Top Tumbler No. 1</p> 	<p>Top Tumbler No. 2</p> 	<p>Top Tumbler No. 3</p> 
<p>Bottom Tumbler No. 1</p> 	<p>Bottom Tumbler No. 2</p> 	<p>Bottom Tumbler No. 3</p> 
<p>Top Tumbler No. 4</p> 	<p>Top Tumbler No. 5</p> 	<p>Top Tumbler No. 6</p> 
<p>Bottom Tumbler No. 4</p> 	<p>Bottom Tumbler No. 5</p> 	<p>Bottom Tumbler No. 6</p> 
<p>Springs</p> 	<p>Retainers</p> 	<p>Retainers</p> 
<p>Retainers</p> 	<p>Retainers</p> 	<p>Fig. 33</p>

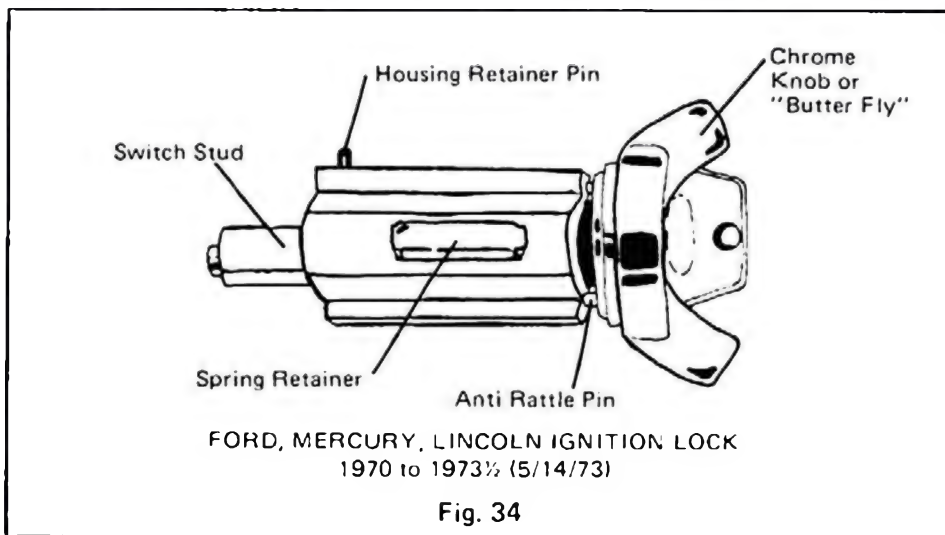
Another method of decoding the key is by placing the bottom pins one at a time back into the cylinder, and using a depth key to determine their length. For Ford lock systems, a set of five depth keys are needed. Each key has a series of number one cuts or number two cuts, etc., on up to the number five cut. Chrysler depth keys utilize six keys, each one having a number one cut or a number two cut or a number three cut, etc., on up to the number six cut. Depth keys also indicate the spacing between the tumbler cuts, which would be very helpful in impressing keys. The method of determining the cuts would be by placing the bottom pin back into the lock cylinder, and testing each depth key until the plug moves freely in the cylinder. Care must be used to go from the number one cut depth key to the number five cut depth key in progression. Otherwise, you could read the key incorrectly. It would also be helpful if you used a paper clip to push down on the bottom pin while the key is inside to make sure that the bottom pin is seated properly on the depth key.

It is also possible to compare pin tumblers with those that are supplied in a pinning kit. A pinning kit has all of the items indicated in figures twenty eight and twenty nine, and the tumblers are clearly marked so that comparison can be made with either the driver pin or the bottom pin.

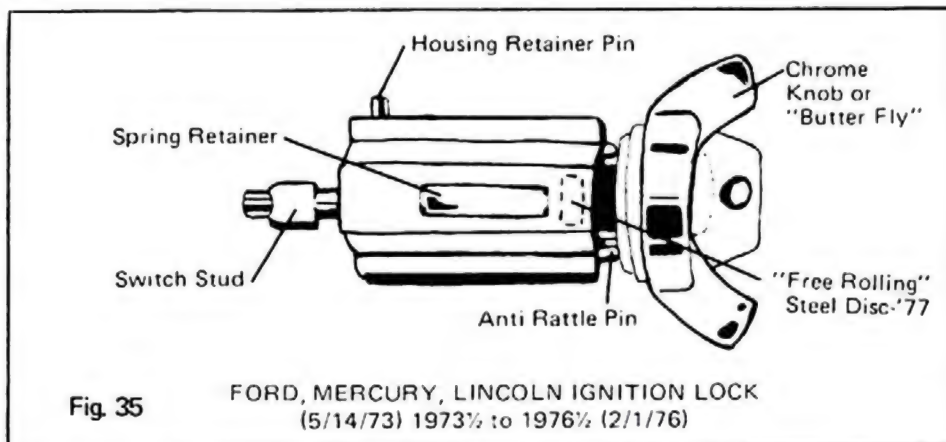
After decoding the key, it is a very simple process of cutting the key with a key cutter, or if you have no key cutter, by using a blank and a depth key to cut the proper code. Using the depth key and a blank, use a pair of vise grips to hold them together while you make impression marks with a number four Swiss file. After you have your impression marks file the marks to the depth desired, by comparing them with the depth keys every so often.

Locksmith Techniques For Ford Motor Ignitions

Late model Ford Motor products have three ignition systems. Figure number 34 depicts the Ford, Mercury and Lincoln ignition locks from 1970 through 1973½. Figure number 35 depicts the ignition Ford produced on May 14,

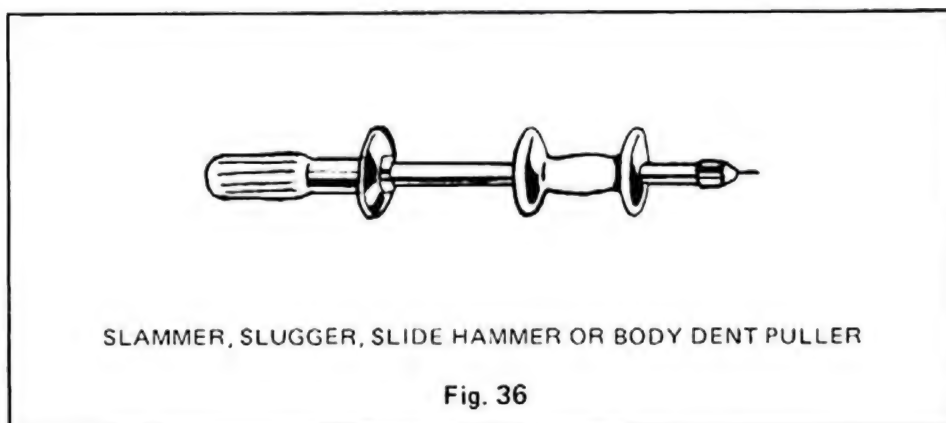


1973. There are several differences in these two locks. The 1973½ through 1976½ model has a square shaped switch stud where the pre-73½ model has a triangular shaped switch stud. The cylinder retaining pin on the 1973½



through 1978 lock has twice the circumference of the pre-73½ models.

These two Ford ignition locks can be removed without too much difficulty by utilizing the slammer, also referred to as the slide hammer, slugger or body dent puller (figure number 36). The model depicted is manufactured by Snap



On Tools. If you can find them, 3/8 by 2" hex head screws are recommended as the extra ½" length allows you to use the slammer on General Motors ignitions. More about that in the next chapter.

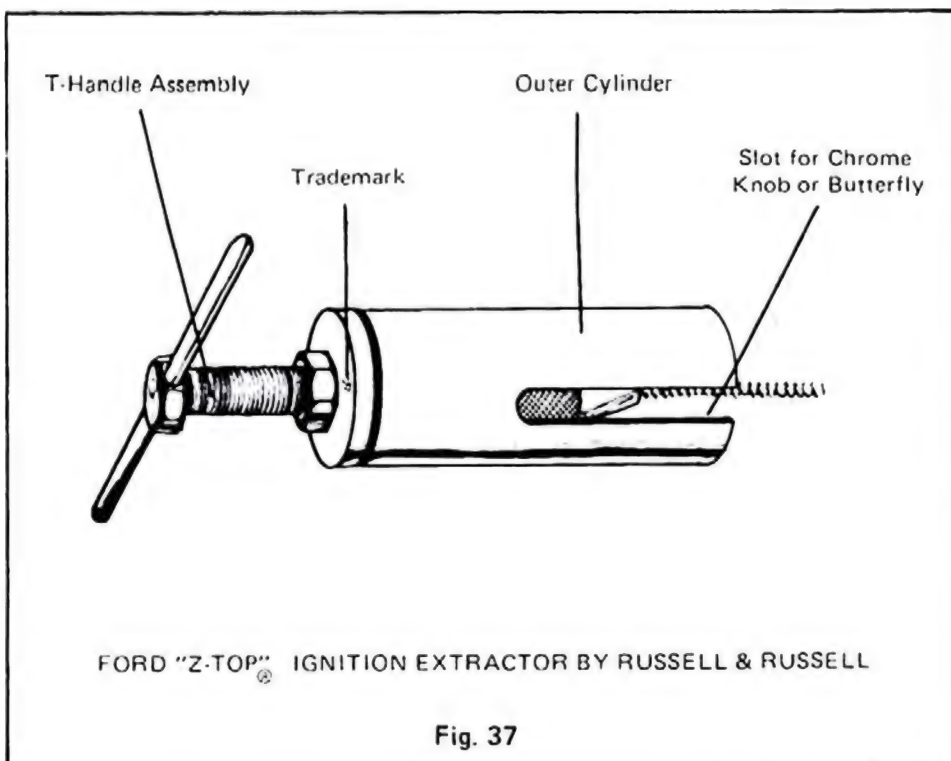
The method of removing Ford Motor locks with the slammer is, quite simply, to screw the slammer into the keyway of the ignition approximately ½" and pull back on the slide hammer with force. A couple of raps should take out

the 1970 through 1973½ ignitions and a few more raps will take out the 1973½ through 1976½ ignitions. Occasionally, the chrome knob or butterfly will come off leaving the ignition still intact. If this should happen, simply remove the left anti-rattle pin (the one closest to you as you sit in the driver's seat) and screw the sheet metal screw of the slammer into the cavity. I make this suggestion because it is rather difficult to screw the screw into the keyway of the core once the butterfly is removed and also because the retainer pin situated at the rear of the lock is directly behind the brass anti-rattle pin that has been removed. Inserting the screw into the anti-rattle pin cavity applies direct contact to the housing retainer pin and therefore, makes it easier to extract the ignition. The slammer does make quite a bit of noise, and it is advisable that the windows be rolled up on the vehicle to deaden the sound. Some people put rubber washers between the slide hammer and the impact nut to deaden the sound, but I feel this is unadvisable as you lose "impact". Once the lock is removed, insert a flat head screw driver into the "star gear" cavity and turn clockwise to start or install a new lock.

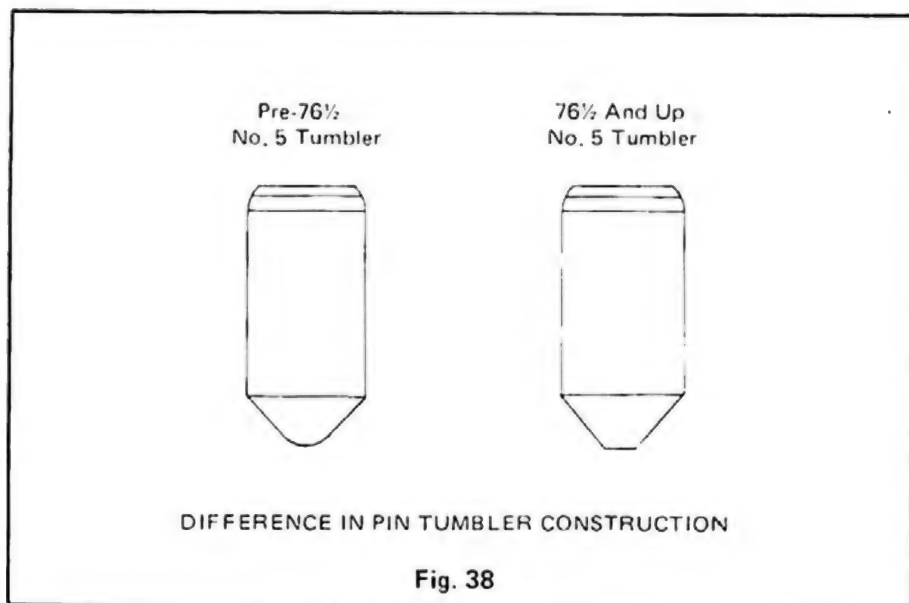
It is possible to by-pass the 1970 through 1973½ Ford, Mercury and Lincoln ignitions by the use of a "twist key". The twist key is made by taking a brass chrome plated blank (it is important that it be made of the strongest material possible and a good plated key will suffice) and making a series of number three cuts on one side of the blade. Utilize your key cutter to cut the blank or use your depth keys and a number four Swiss file. You may wish to ask your local locksmith to cut these for you. Only cut one side of the blade as this will make the blank stronger. Insert the blank into the Ford lock with the cut portion toward the tumblers inside the lock (in Ford products the tumblers are usually situated on the bottom of the keyway and the key would be inserted with the cut portion downward). After the key has been inserted into the lock, take a pair of channel locks and grab the "ears" of the chrome knob or butterfly and the key. By using constant, steady force, twist the key to the "start" position. It is important that your channel locks be able to hold both knobs and the key and that only a steady, constant force be used. If you fail to grab both knobs and use a jerky twisting method, it will break the key and the chrome knob will come off. If this happens, remove the anti-rattle pin and remove the ignition with a slammer or Ford extractor. The twist key method is possible because of the construction of this Ford lock. The cylinder is constructed of pot metal and the number three cuts push the pin tumblers up into the plug housing. Under torque, the tumbler housing and the tumblers themselves bend so that it is possible to turn the plug. Occasionally, the twist key method makes the ignition stick and the starter will continue to turn after the engine has been started. When the twist key makes the ignition stick, back the key towards the "off" position and you should have no further problems. The twist key method does not work

well on the 73½ through 76½ year ignitions as the chrome knob or butterfly is only lightly staked on the plug flange. Occasionally, it will work, especially if you turn the key only to the "on" position and do not try to push it to the "start" position. In the "on" position the lock on the steering wheel is released. Start the car by hot wiring or tow it.

Perhaps the easiest method of removal of the 70 through 73½ and 73½ through 76½ ignitions is by utilizing the Ford Ignition Remover Tool. To use the tool, an outer cylinder is placed over and around the chrome knob or butterfly, a T-Handle assembly with a self-tapping screw is then screwed into the ignition and the lock is then ratcheted out. I will give you a word of caution on purchasing Ignition Extractors. There are several on the market, and the majority of them are poorly constructed or too time consuming to utilize. Shop around carefully and purchase only those tools that are guaranteed and in the middle or high price range. There are several Remover Tools that are in the lower price range and you will get exactly what you pay for. Below is the Ford Ignition Extractor that I have developed. It operates on the same principal as the slammer. It is easy to operate, quiet and can be used by locksmiths as a "nose puller" on safety deposit boxes. This model decodes hundreds of other locks including foreign automotive ignitions.

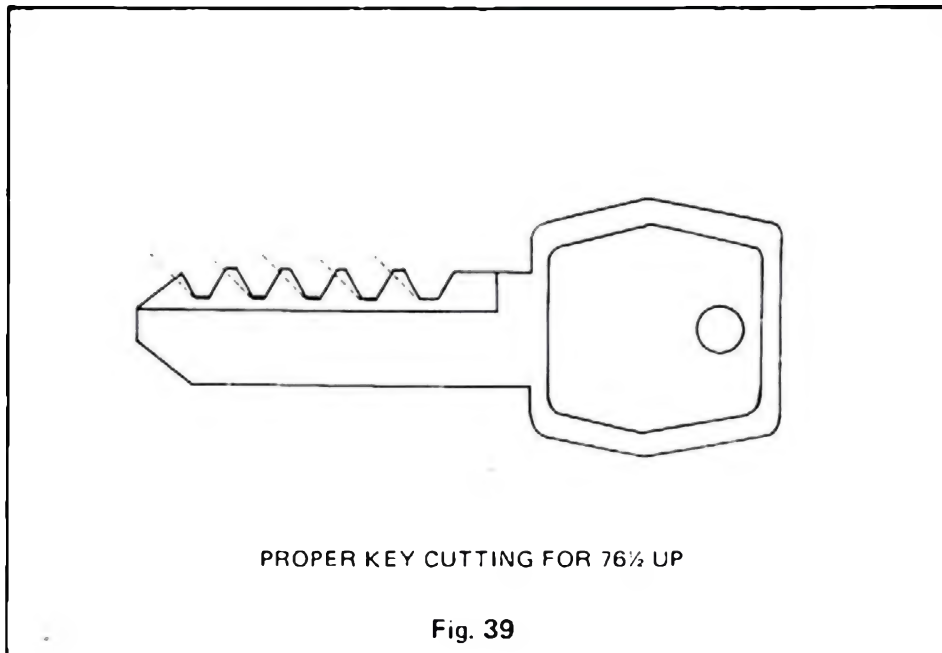


On February 1, 1976, Ford came out with a new ignition. In 1977 they altered this ignition somewhat. The new ignition is very similar to the 73½ through 76½ ignition in figure number 35, but there are some differences. Not all 1976 cars have this type ignition and it depends upon when they were produced. Cars produced after February 1, 1976 may have the new ignition. Economy cars, such as the Pinto, Maverick and Mustang II will more than likely have this type of ignition. It is very difficult to slam these ignitions or remove them by using a Ford Remover Tool. Using the slammer method, it took over fifty pulls of the slammer to remove the ignition! While using the Ford Tool, I had to replace the screw five times before the lock would come out! The first difference in the new 76½ to 78 lock is the construction of the pin tumblers. They are now constructed of a slightly harder metal alloy instead of brass to impede the "twist key" method and drilling. The bottom pin tumblers on the pre-76½ Ford locks have a slight point at the tip. The new alloy number five bottom tumblers have a flat place on the tip to impede "rake" picking (refer to figure number 38). Cutting a key for these new locks



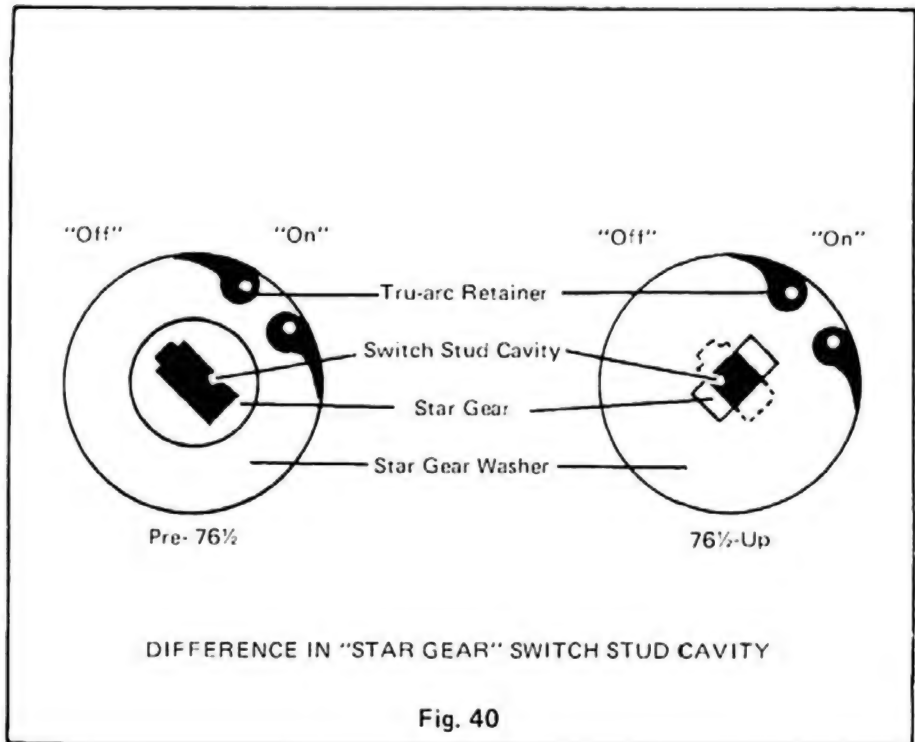
in the regular methods will not work because of the flat spot. In fact, Curtis Industries has come out with a new model Ford key cutter for cutting 76½ through 78 keys. However, it is still possible to cut a key with your old cutter by making the slopes or hooks of the cuts less acute (see figure number 39). The flat spot on the pin tumbler does not ride up the slope as well as the pointed tumbler does. You will find that the key will work rather well, but will not come out of the keyway without using a pair of pliers. To combat this, after you have cut the key on your key cutter, recut it by moving it approximately 1/16" backward so that the cuts overlap making the slopes less

acute. The key should then work perfectly.



The next difference is the spring retainer and spring retainer housing. The spring retainer is similar to those found on Dodge Colt vehicles depicted in the bottom left square of figure number 32. Incidentally, these Chrysler retainers can be used when servicing this type of lock. The spring retainer housing is recessed into the shell of the lock and is not exposed as the pre-76½ and up models. This tends to strengthen the spring retainer housing and impedes the twist key method. On the newer 1977 and up ignitions, (those 76½ model locks in 1976 Fords do not have this) there is an armour plated, "free rolling" steel disk situated in the shell or outer cylinder just before the spring retainer (refer to figures number 31 and 36). This "free rolling" steel disk impedes drilling the tumblers at the shear line as the tip of the drill causes the steel disk to rotate when attempting this. The core of locks possessing steel disks are slotted and the steel disk fits into this slot. This retains the core in the outer cylinder so that the core cannot be removed without the shell and impedes "shimming".

The switch stud of the 1976½ and up model ignition is similar to the 1973½ through 1976 model depicted in figure number 35. The only difference is that the switch stud is slightly longer. In years previous to the 76½ model, the switch stud of the ignition fit into a "star gear" at the base of the housing cavity that was retained by a circular washer. The 1976½ and up model has a slotted washer that retains the star gear that will not allow the switch stud to pass through it unless it is in the "on" position. In the "off" position,



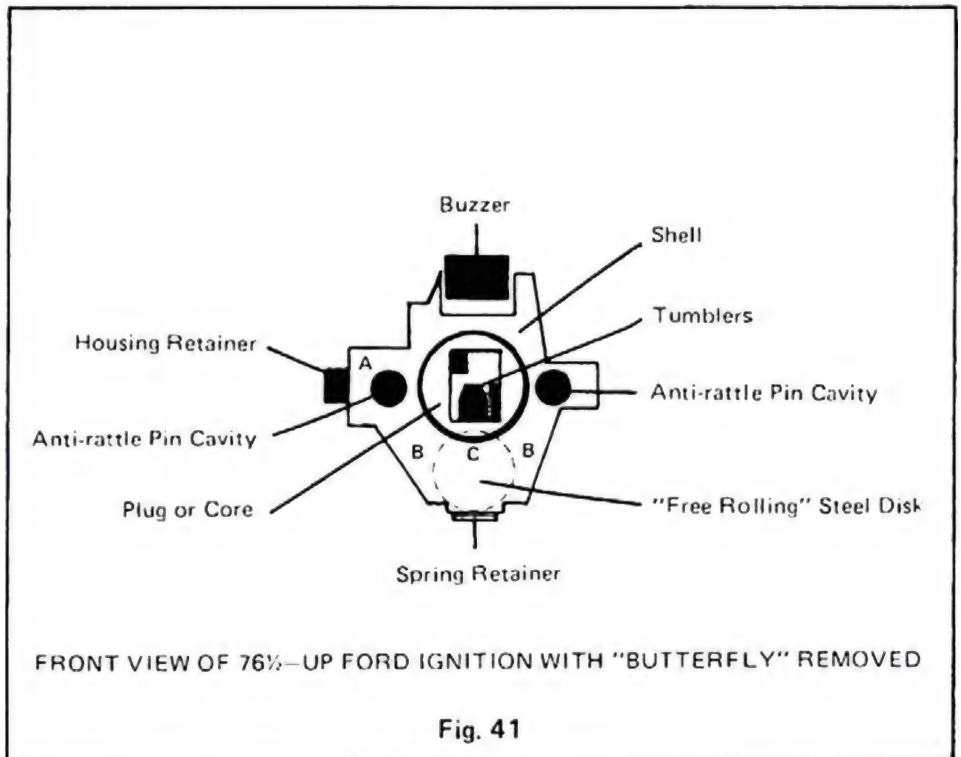
the slotted washer will bind against the switch stud (refer to figure number 40). This double retention of the lock is what makes it so difficult to remove with a slammer. If you do succeed in slamming the ignition out, in all probability the switch stud will have broken off inside the slotted washer. In most cases, the slotted washer will be bent and the star gear will have slipped off track making it impossible to start the vehicle. In some cases the star gear does not slip off the track and if the broken portion of the switch stud is long enough it is possible to start the ignition by turning the broken switch stud to the "start" position. If you are lucky the car will start. If not, you may have been lucky enough to have at least released the wheel from the "locked" position and if so, can hot wire the car or drag it off. If the wheel is still in the locked position, it will be necessary to remove the slotted washer, the star gear and the broken switch stud. The slotted washer is retained by a tru-arc retainer that can easily be removed with a pair of tru-arc pliers or sharp pointed needle nose pliers. Once you have removed the slotted washer and the star gear, you will be able to see the track that the star gear pushes forward to start the vehicle. You can push this track forward with a screw driver to start the vehicle. Care should be taken when replacing the star gear that it be on the track correctly. To align, push the track backwards to the "locked" wheel position and match the threads of the track to the star gear. A little trial and error should enable you to determine the correct position.

Make sure it is correct before you replace the ignition or you will have to start all over again by removing the ignition. Because 1976 Ford products could have either the 73½ through 76 or the 76½ through 78 ignition, it would be wise to look through the keyway at the tumblers. If the tumblers are a dull gray steel color, you may not wish to use a slammer or Ford puller because this is the 76½ through 78 ignition.

Because of the new anti-theft features, it is difficult to rapidly extract the 76½–78 Ford ignition. For that reason, I suggest removal of the door lock to decode the tumblers and cut a key or picking the lock. The door lock can be impressioned, however, the flat tips on the alloy tumblers make it difficult to impression the ignition. Removing the door lock by the methods previously discussed in this chapter is quicker than impressioning and is a skill easily mastered. On the more expensive Ford, Lincoln and Mercury cars, such as the T-Bird, Lincoln and LTD, etc., the door lock clip is exposed in the jam of the door and can easily be removed in seconds with a screw driver.

The Ford ignition lock can be removed by using a Ford Extractor, a slammer and/or drill in the following methods. I highly recommend Black and Decker's new cordless drill as it is comparatively inexpensive for locksmithing work. The rechargeable battery pack accepts several Black and Decker accessories and you might consider purchasing the spotlight also. The low RPM output of the Black and Decker drill does not break drill bits as often as a high speed drill would in lock servicing. Use only the best carbon steel (carbide drill bits) you can find as they are less apt to break than the "cheapies". If you break a bit while drilling, you have created another obstacle for yourself and it is suggested that you practice drilling procedures on old locks before using them in the field.

Ignitions of Ford Motor products with a tilt wheel are easier to remove than others. On the column, near the four way emergency flashers there is a small hole. At the bottom of this hole is the housing retainer pin of the ignition. When the lock is turned or picked to the "on" position, the retainer pin can be depressed with an ice pick enabling you to remove the ignition by pulling it outward with your hand. To remove the ignition in the "locked" position, use a 1/8" carbide drill bit to drill out the housing retainer pin through the access hole. It is important to keep the drill as straight as possible and it is only necessary to drill 3/16" into the housing retainer pin to free the ignition. Another method would be to "punch" the housing retainer pin into the core. Insert a 4" piece of welding rod into the access hole and tap the end sharply with a hammer until the retainer pin is driven forward into the core allowing you to remove the ignition. These methods work well with pre-76½ model Ford ignitions that are not retained by the "switch stud". Pre-76½ year model ignitions can be drilled out in several ways. The first is to remove the



chrome knob or butterfly with a pair of channel locks. After removal of the butterfly, remove the anti-rattle pin to the left of the core (marked "A" in figure number 41). After the brass anti-rattle pin has been removed use a broken key extractor from your pick set to remove the small steel spring behind the anti-rattle pin. Using a 3/16" carbide drill bit, drill a hole 1 1/4" long slightly to the left of the anti-rattle pin until the housing retainer pin has been sheared. If you desire, you may use a larger drill bit and drill through the anti-rattle pin cavity. It is then possible to remove the ignition by pulling outward on the chrome knob. If the lock resists, you have not properly sheared the housing retainer pin where it intersects with the shell and the column housing. If you have in fact drilled through the retainer pin, it is sufficiently weakened so that you can extract it with either a slammer or a Ford extractor.

The second method would be by drilling the tumblers. Using a 3/16" carbide drill bit, drill a hole 1 1/8" long through the tumblers at the point where the shell and the core meet (marked "C" in figure number 41). It is important that you keep the drill as straight as possible and do not exert too much pressure on the drill or your bit could break, creating another obstacle. As you drill, you will feel the drill penetrate each tumbler. As you drill through a tumbler, the drill may "surge" and unless you release the pressure immediately, you could break the drill bit. Once you have drilled to the required depth,

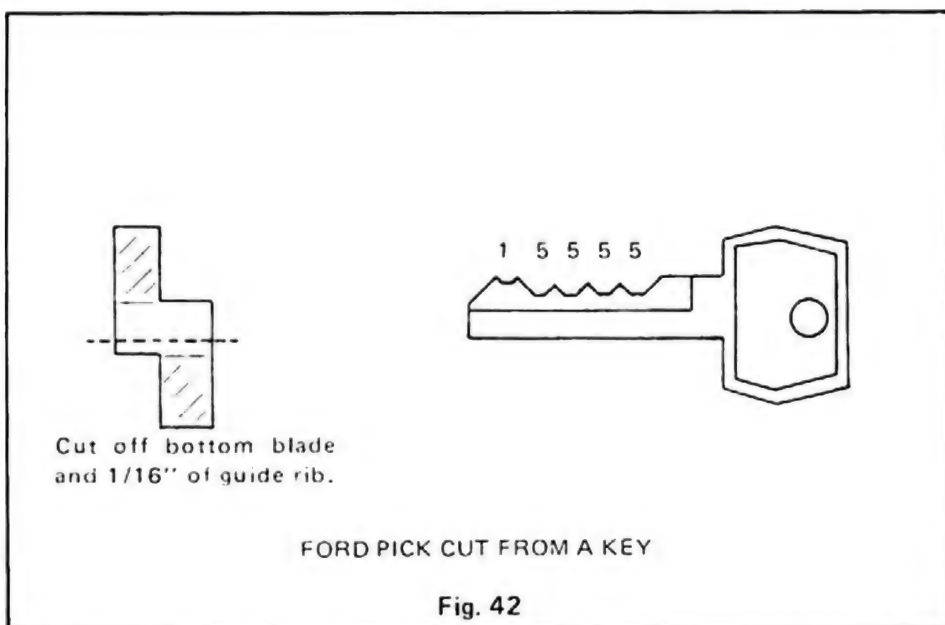
you have created another shear line, allowing you to turn the core or plug to the "start" position. Later, the lock can be extracted in the usual methods. It is also possible to turn the Ford ignition to the "start" position by using a piece of "shim stock" (small strips of metal of ten thousandths thickness or less). After the chrome knob or butterfly has been removed, insert a shim (feeler gauges work nicely) between the core and the shell of the lock at the point marked "C" in figure number 41. Using the curved hook pick, depress each tumbler as you push the shim stock forward with your other hand so that the shim stock separates the top and bottom tumblers. Once each pin has been separated, it is possible to turn the core or plug to the "on" position by inserting a flat head screw driver into the keyway and turning the plug clockwise.

It is possible to shim the 76½ year model Ford ignition as previously described, provided however, that it is not the type that has the "free rolling" steel disk. The free rolling steel disk is usually found only on 1977 and 1978 model ignitions. To shim the tumblers or drill them out, it is first necessary to remove the steel disk by drilling two 3/16" holes into the shell of the lock 1/4" deep on either side of the disk (marked "B" on figure number 41). This steel disk is approximately 5/16" in diameter, so space the holes accordingly. Once the holes are drilled, insert a flat head screw driver between the shell and the column housing (at the point marked "spring retainer" on figure number 41) and pry up to remove the shell covering the steel disk. Be sure that the holes you have drilled have sufficiently weakened the shell so that prying the shell out does not damage the column housing. Once the small portion of the shell has been removed, use a broken key extractor to remove the steel disk and shim or drill as previously described. Once the ignition has been turned to the "on" position, the lock can be extracted by drilling out the column housing retainer pin or by using the slammer or Ford Extractor. Although I have not tried it, it would be possible to drill a 3/16" hole through the keyway 1 3/4" deep to sufficiently damage the switch stud so that the lock could be extracted with the Ford Extractor or slammer. The only problem would be the numerous obstructions in the keyway that would make it easy to break the drill bit without great caution.

As previously stated, drilling a lock takes a certain amount of skill and patience. The deeper you drill into a lock the more difficult it gets, as broken tumblers and other debris are apt to break the drill bit. Caution should be used so that you do not "over drill" and put holes where they should not be. To prevent this, paint marks on your drill bit, or better yet, place small pieces of copper tubing around the drill bit to expose just enough of the drill bit to match the depth of the hole you wish to drill. The copper tubing also helps to strengthen the drill bit making it less apt to break. Ford locks can be "riddle drilled" by drilling 1 3/8" holes with a 3/16" drill in the shell of the

lock above and below the anti-rattle pin cavities at the shell's thinnest points.

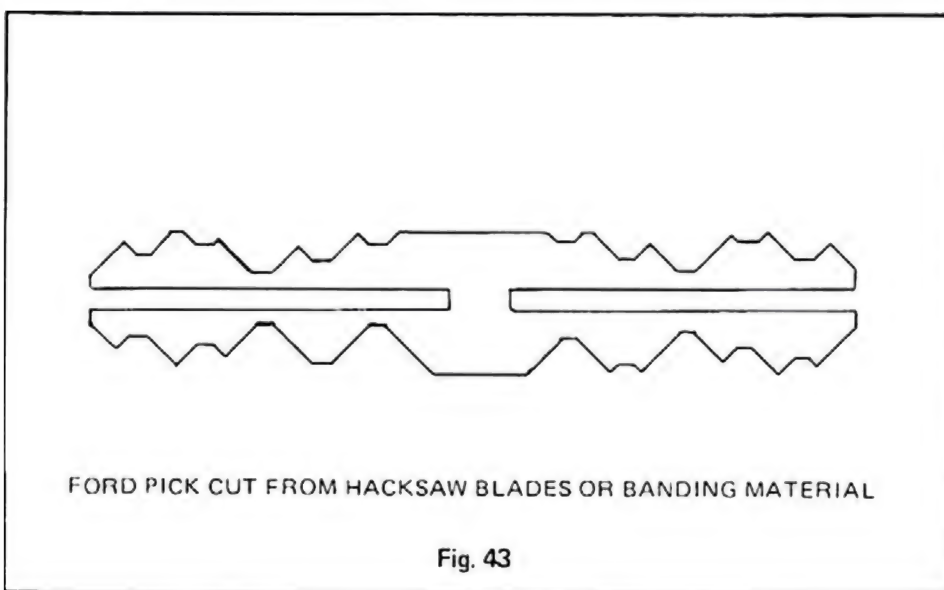
Generally, only three or four holes are necessary to sufficiently weaken the lock so that the core can be turned and the shell removed "piece by piece". Drill jigs are a good thing to have, as they aid the locksmith in determining where to drill and aid in keeping the drill bit straight during drilling. I have made a set for myself out of wood. After shaping the jigs, I drilled holes in the wood at the necessary drill points and inserted "sleeves" made of copper tubing to protect the drill jigs during drilling. Copper tubing can be held in place by using epoxy or super glue or by slightly flaring the ends of the copper tubing with a punch.



As stated in the first chapter, Ford locks can be easily picked. The handy Ford pick depicted in figure number 42 is easy to make and enables you to pick Ford locks faster than utilizing regular picks. To construct the Ford pick, cut the depths five, five, five, five, one from bow to tip on an ordinary double sided Ford key blank on one side only. Next, grind the uncut blade flush to the guide rib. Then grind an additional 1/16" of the guide rib away, and your Ford pick is ready to use. Insert the key into the keyway and use a raking motion while lifting up and down on the bow of the key. With your free hand grasp the "ears" of the butterfly or chrome knob and apply alternate tension while continuing in and out, up and down, raking and picking until the ignition turns over to the "on" position. Nine out of ten times this Ford pick will turn the ignition over in anywhere from thirty seconds to three minutes. I made several other Ford picks with two, three and four cuts instead of the one cut. Whenever the one cut fails to work as fast as I would

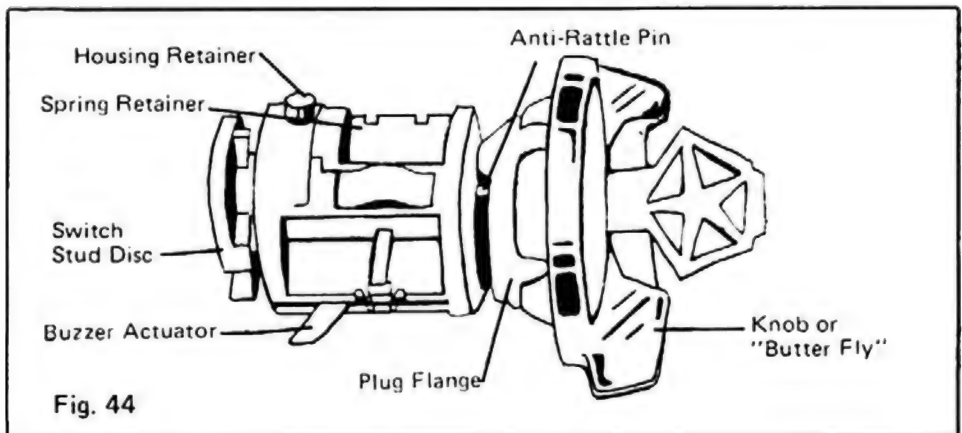
like it to, I progress from the second to third to fourth pick until the lock turns over.

Figure number 43 depicts another set of Ford picks that can be constructed out of old hacksaw blades or banding steel. Using a key cutting machine, any variation or combination of codes can be cut into the pick. The pick should be about six or seven inches in length (please note that figure number 43 only depicts the picking ends - there should be about six inches in length separating the two picking ends so that you can properly grasp the tool). After the picks have been cut to the cuts you desire, file or cut a slot down the middle of the pick. This slot provides some "spring" to the pick. Use an undulating and back and forth motion while applying alternate tension pressure on the chrome knob with your free hand.

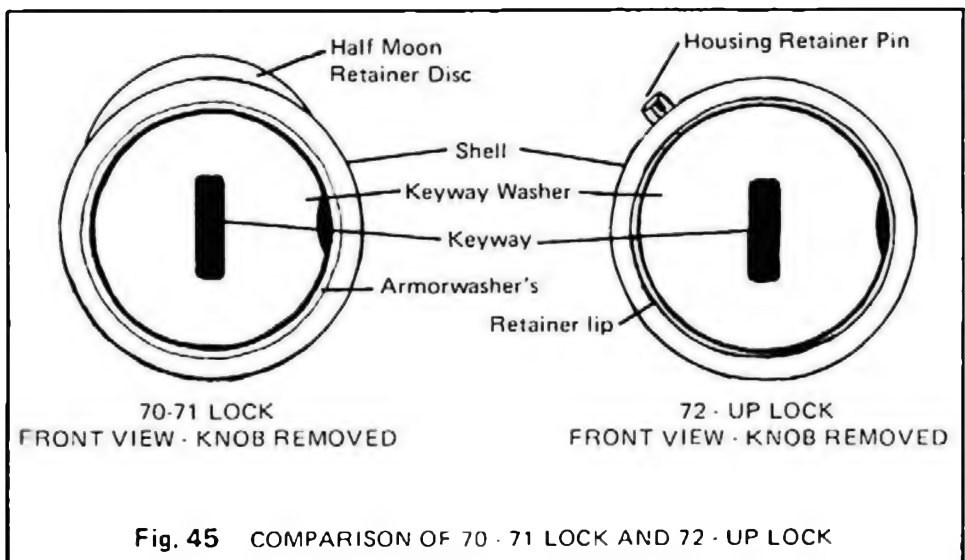


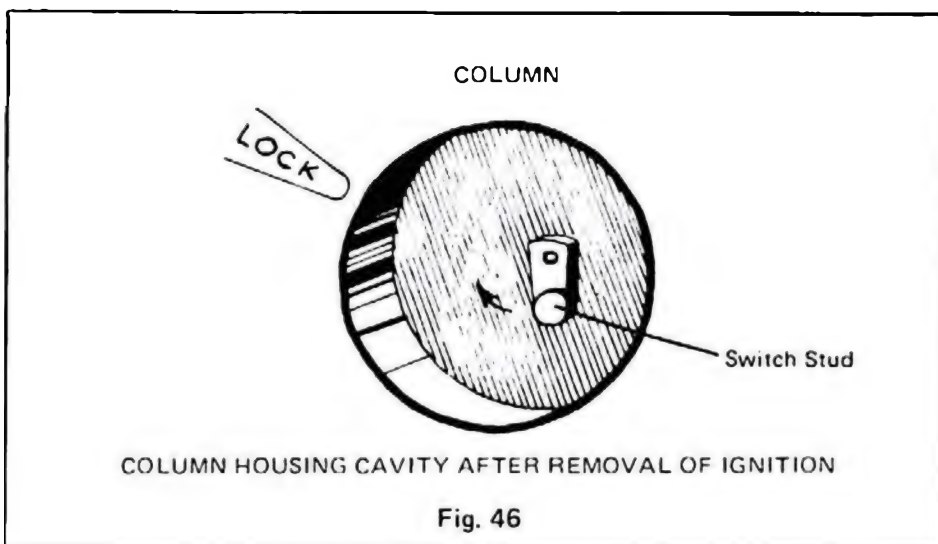
Locksmithing Techniques For Chrysler Motors Ignitions

Chrysler Motors utilize three types of ignitions on their late model American made automobiles.

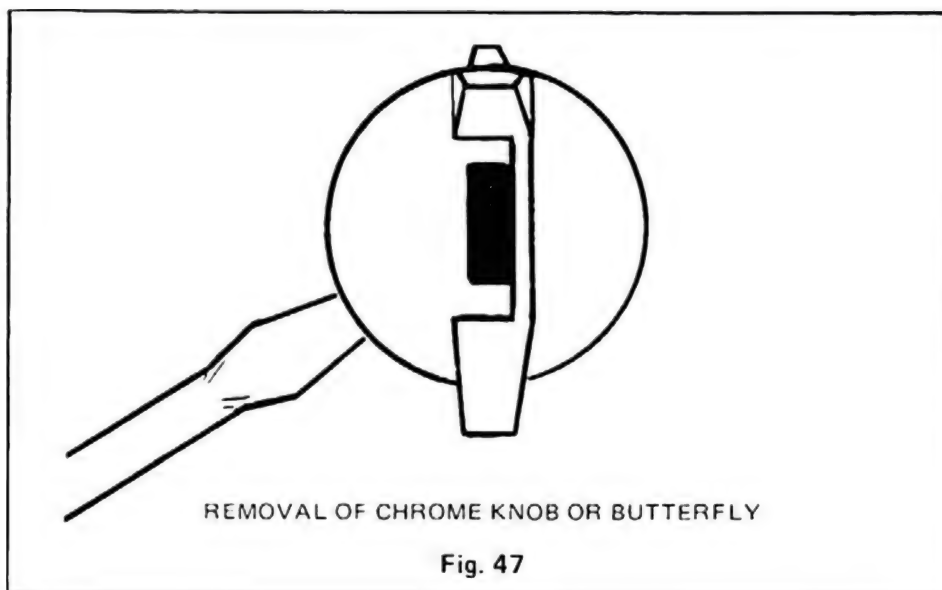


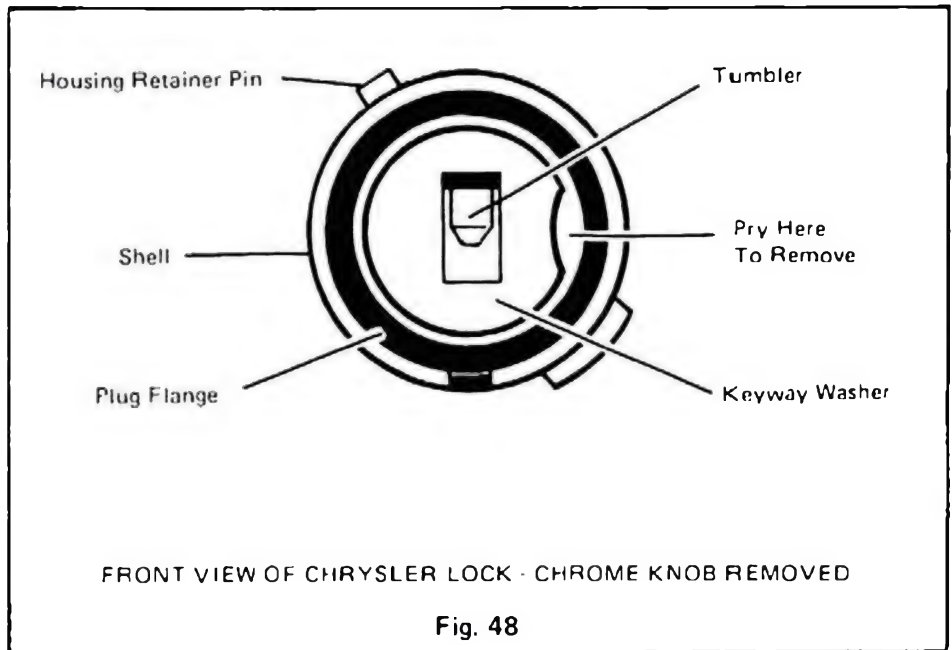
In 1970, Chrysler came out with their first steering column ignition lock with three way locking. Located on the column, it not only locks the ignition switch but also the steering wheel and transmission as does the Ford ignition previously discussed. This ignition used a half moon retaining disc to hold the cylinder in the housing. For some reason Chrysler discontinued the use of this particular model in 1970 and in 1972 came out with a lock that used a retaining pin to retain the lock in the column (figure number 44). Your author attempted to purchase a 1970 and 1971 replacement lock and found that they are few and far between as they are produced by only one automotive ignition manufacturer. The retaining pin on the 1972 through 1978 and the half moon retainer disc on the 1970 and 1971 ignitions are both spring loaded and protrude into the void of the column housing cavity. The column housing that holds the lock cylinder is made of pot metal (figure number 46).



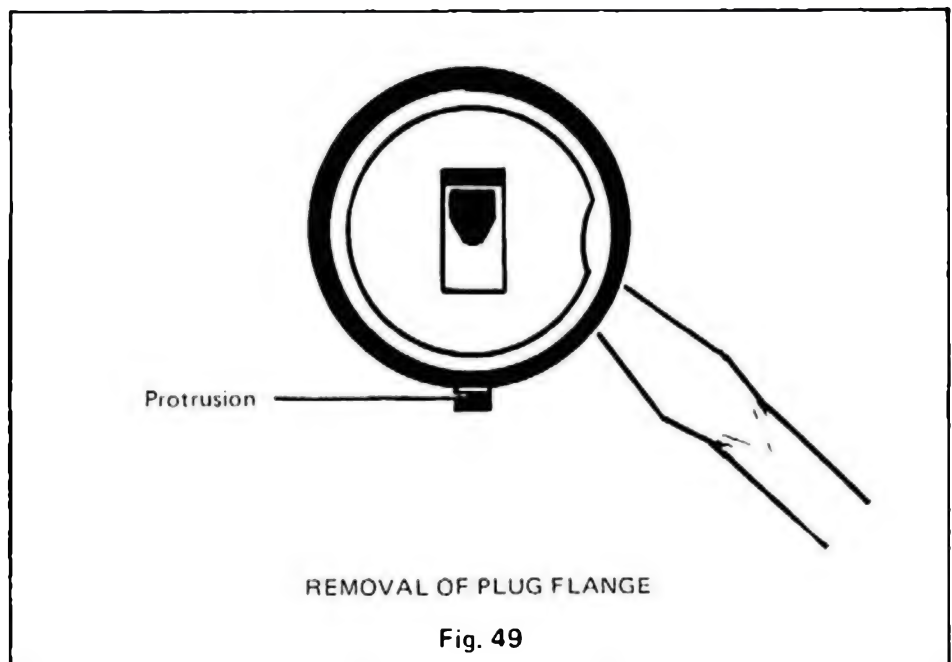


The 1970 and 1971 locks have an armor washer. The washer prohibits screwing the self-tapping screw of the slammer into the ignition. However, the armor washer can be removed by using a sharp pointed screw driver, after first removing the chrome knob or butterfly with a screw driver (figure number 47). After discovering that the Chrysler ignition has an armor plated washer (usually it has a dull, dark greyish color) take a sharp pointed screw driver and peel away the armor washer's retainer lip by starting at the small slot that is located at the 2 o'clock position of the lock. This operation is easy and can be done with hand pressure without the use of a hammer as the armor washer's retainer lip is of soft pot metal (figure number 48). After the armor washer has been removed place the self-tapping screw of the slammer at the top of the keyway and screw it in no more than 1/2". Otherwise, it will depress the buzzer actuator. When the buzzer actuator is depressed, it

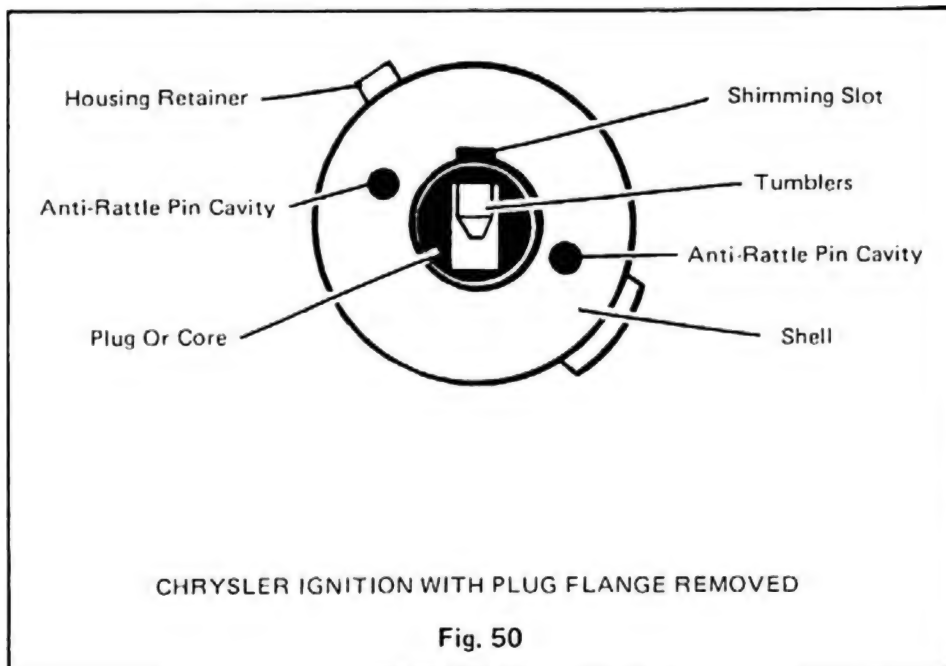




protrudes into the column housing and will help retain the lock during extraction. Occasionally, the tumblers of the lock force the slammer screw downward so that it depresses the buzzer actuator. To avoid this, use a paper clip bent at a 45 degree angle to raise the tumblers with your free hand while screwing the slammer into the keyway. An easier method would be to pry off the plug flange, after removal of the butterfly, by prying upward with a screw driver after placing same between it and the column housing (figure



number 49). After removal of the plug flange, remove the anti-rattle pin situated at the 10 o'clock position in the shell of the lock (figure number 50). Next, screw the self-tapping screw of the slammer into the anti-rattle pin cavity. It is best to use the anti-rattle pin at the 10 o'clock position as it is closer to the retainer pin and exerts direct pressure on it during extraction.



After the self-tapping screw is in place, extract the lock by slamming away as hard as possible, keeping the slammer as straight as you can. A quieter and more professional method would be to use the Ford Extractor depicted in the previous chapter instead of the slammer.

The 1972 through 1978 Chrysler ignition usually does not have an armor plated washer, and appears to be made of a chrome colored alloy. It still can be difficult to screw the slammer and the Ford Extractor into this washer and it can be removed in the same manner as the 1970 and 1971 washer.

Neither of these locks slam easily. Oftentimes, it is necessary to slam the ignition as many as ten times. For that reason, I would suggest using the Ford Extractor or Chrysler Extractor. Occasionally, the column housing is damaged during extraction at the point where the housing retainer pin fits into same, especially when using the slammer. When this happens, the replacement lock will not fit properly, (the hole in which the housing retainer fits is "torn" allowing the lock to move backward and forward with about 1/4" play). If this happens, put a few drops of super glue on the shell of the lock so that it adheres to the housing itself.

Standard Chrysler (pin type) ignitions can be easily "shimmed". Remove the plug flange with a screw driver as previously described. Next cut a piece of shim stock of .005 thickness (feeler gauges work well) 2" in length and slightly less than 1/8" in width. Insert the shim in the slot of the shell above

the pins depicted in figure number 50. Next insert your curved hook pick, that is available in most pick sets, into the keyway and press each tumbler up while pushing forward on the shim stock with your free hand. One by one, you will be able to separate each tumbler at the shear point. After the shim has traveled into the lock approximately 1" deep, all the pins have been shimmed. Next, use a small screw driver or tension wrench and insert same into the keyway and apply a clockwise tension. The core should turn slightly. It is then necessary to use the hook pick to depress the buzzer actuator at the bottom of the keyway so that the core or plug will turn. After some practice, it is possible to shim the lock in less than one minute. Later, the lock can be extracted in any of the methods previously discussed. Another method of shimming would be to utilize shim stock of .0025 thickness and insert same between the core and the shell above the tumblers. The width of the shim stock should not exceed 1/2". Use the same method as described above to pick each tumbler and shim the lock. When shimming or picking any lock, a small shot of WD-40 helps loosen gummed-up tumblers.

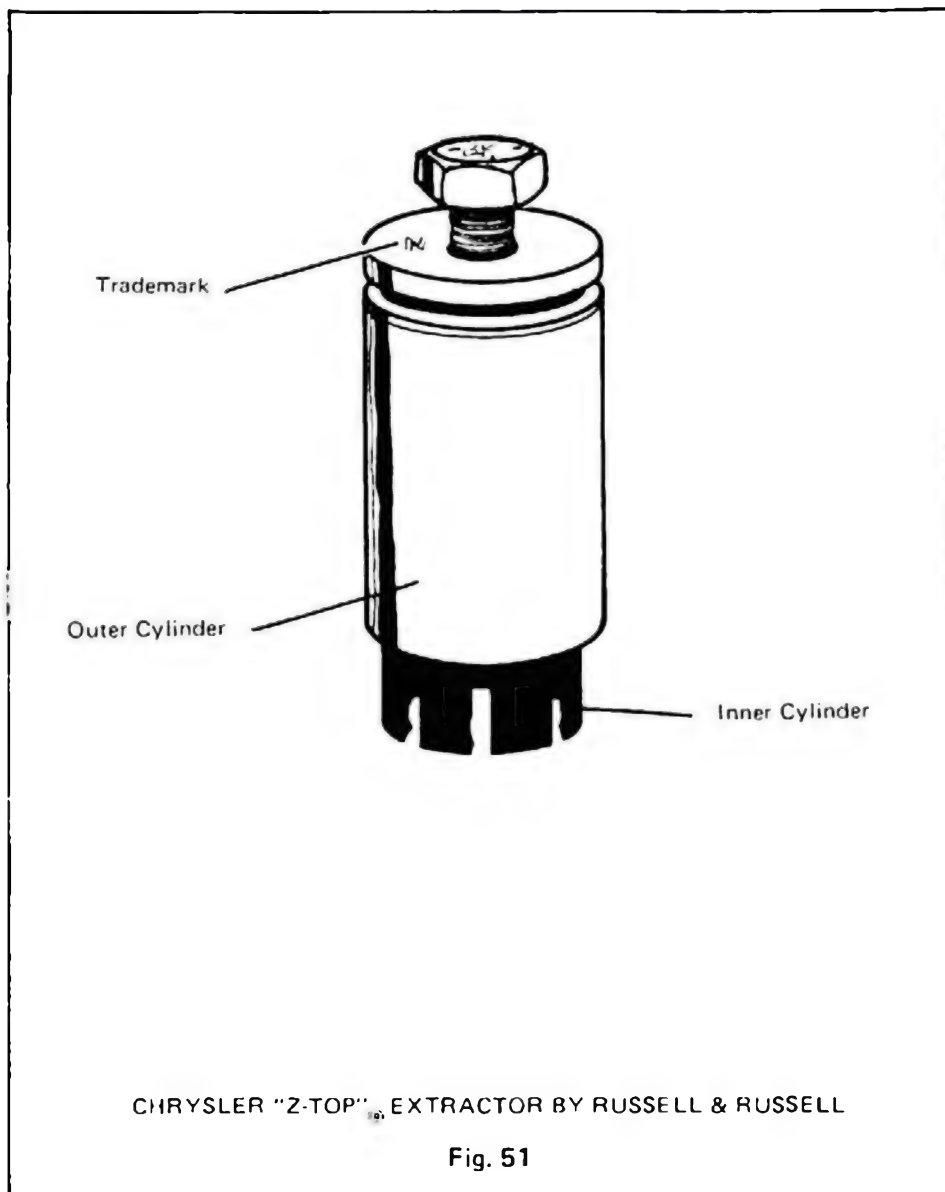
Standard Chrysler locks are easy to pick and I have had great success with curved hook picks and the Lock Aid Pick Gun, the latter is especially good for trunk and door locks.

A new shear line can be drilled into the plug and shell to enable you to turn the ignition to the "start" position. Using a 3/16" carbide drill bit, drill a hole 1" long at the "shimming slot", (figure number 50) so that the drill cuts into the shell and the core. After you have drilled the hole and removed the debris, place a small screw driver or tension wrench in the keyway of the core and turn clockwise to the "start" position. Remember to depress the buzzer actuator so the core or plug will turn freely. Remove the lock later in the methods previously described.

Perhaps the easiest method of extracting Chrysler ignitions is by utilizing a Chrysler Extractor. To operate the Chrysler Extractor, the chrome knob or butterfly is removed and the inner cylinder of the Extractor is snapped onto the plug flange. The inner cylinder consists of eight splines or fingers with "grabbing hooks" that are contoured to the shape of the Chrysler plug flange. After the inner cylinder is securely in place, an outer cylinder is placed around the inner cylinder and the lock can be ratcheted out in under a minute! There are several Chrysler Extractors on the market and you should use caution when purchasing same. Many of them are poorly constructed and may cause the plug flange to come off instead of extracting the ignition! Sometimes this happens anyway, as the core and plug flange of the lock are constructed of low grade pot metal. Allowing the outer cylinder of the Extractor to rotate during extraction also breaks the plug flange. At the bottom of the keyway on the plug flange, there is a small protrusion that keeps the chrome knob or butterfly from rotating during normal use (figure number 49). When attaching the inner cylinder to the plug flange, this protrusion fits inbetween the splines. During extraction, if the outer cylinder is not held securely with your free hand, this protrusion will catch on the inner cylinder splines, rotating the plug flange and causing it to break off. It is amazing to me that this is not mentioned in the instructions of most of the Chrysler Extractors on the market. For that reason, before purchasing a Chrysler Extractor or any other Extractor, it might be wise to write to the

manufacturer and ask them to send you a set of instructions for your review prior to purchasing their tool. If they are not clear, illustrated, easy to read and understand, chances are the tool is a "bummer".

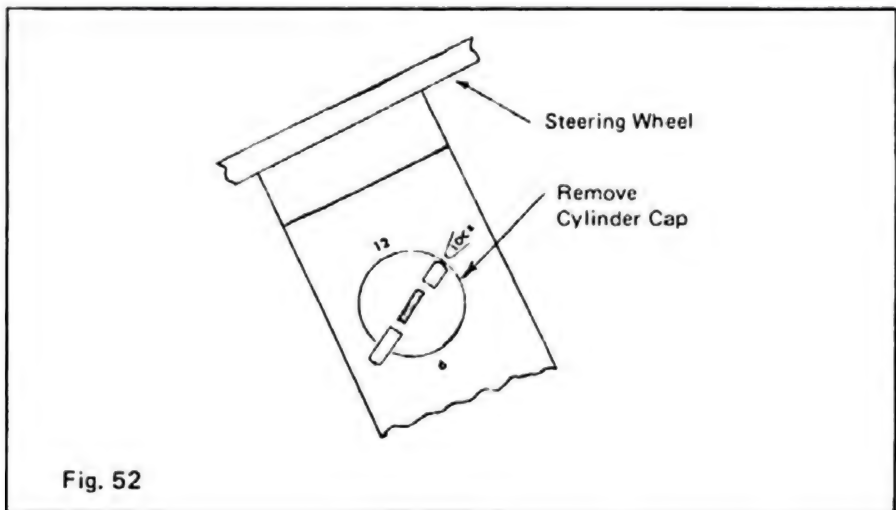
Figure number 51 depicts the Chrysler Extractor that I developed. To combat outer cylinder rotation, this tool uses a thrust bearing (not pictured)to relieve torque. Accompanied with the Chrysler Extractor are a number of small self-tapping sheet metal screws that can be screwed into the keyway prior to extraction to strengthen the plug flange or to reattach the plug flange to the lock if accidentally broken off. After the ignition has been extracted, turn the switch stud depicted in figure number 46 to the left with your finger or a screw driver to start the vehicle.



Another method of removing or extracting the 1970 and 1971 Chrysler lock is by using a .005 or .006 automotive feeler gauge. First it is necessary to remove the chrome knob or butterfly (figures number 47 and 52). Next, insert the feeler gauge between the shell of the lock and the column housing to a depth of approximately 1 3/4 " at the 4 o'clock position (figures number 53 and 54). Then rotate the exposed end of the feeler gauge as though the exposed end was on a pivot, counterclockwise to the 11 o'clock position (figure number 55). This action depresses the "half-moon" retainer disc of the ignition allowing you to extract it with a broken key extractor. Insert the broken key extractor into the keyway so that it "grabs" the tumblers, and pull the lock toward you. If the retainer has been properly depressed, the lock should come out. If you have trouble grasping the lock with the key extractor, pry the lock out with a screw driver. A piece of metal measuring tape can be substituted for the feeler gauge, and the curved shape of the measuring tape fits the curved shape of the ignition lock well. It was rumored that auto thieves were using "butter knives" to remove this type of ignition in the above manner and I presume that is the reason for discontinuing it.

The Chrysler Tilt-Wheel Ignition

Chrysler also utilizes a lock similar to the 1969 General Motors ignition on models having a tilt-wheel. Any of the methods discussed in the next chapter can be used to remove this ignition. After extraction of this ignition, use a pair of needle nose pliers and turn the stud clockwise to start the vehicle.



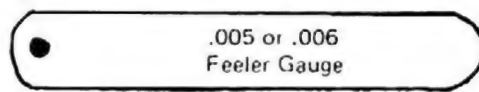


Fig. 53

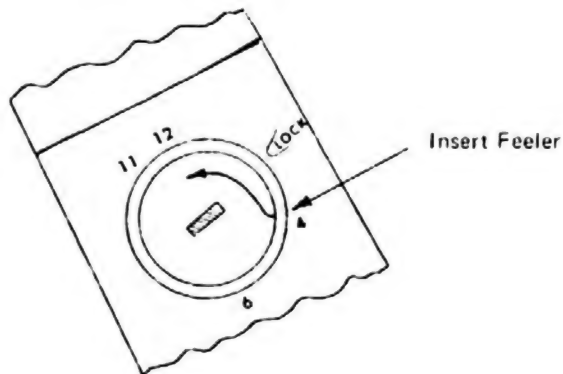


Fig. 54

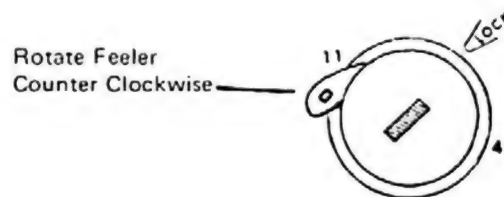


Fig. 55

Chapter III

GM, AM

and Chrysler Tilt Wheel

As previously discussed in this book, the above three ignition systems all utilize a side bar lock. The side bar lock is a modified wafer tumbler system, employing five or six discs depending upon the type, in a series. This type of lock was first introduced in 1935.

Figures six through nine in Chapter One show the principles of operation of the side bar lock. The V notch of the wafer tumbler must be lined by the cut of the key so that the V shaped side bar will fit into it. When this happens, the side bar is clear of the shell, and the plug may be turned.

Cutting Keys By Removing The Tumblers

A standard locksmithing procedure for the servicing of American Motors, Chrysler Motors and General Motors automobiles and trucks, is the removal of and the decoding of the door lock to duplicate the ignition key. Most Chrysler Motors and General Motors vehicles allow easy removal of the door lock by methods discussed in Chapter Two. American Motors vehicles have some models wherein the door lock is encased in the handle mechanism making rapid removal difficult.

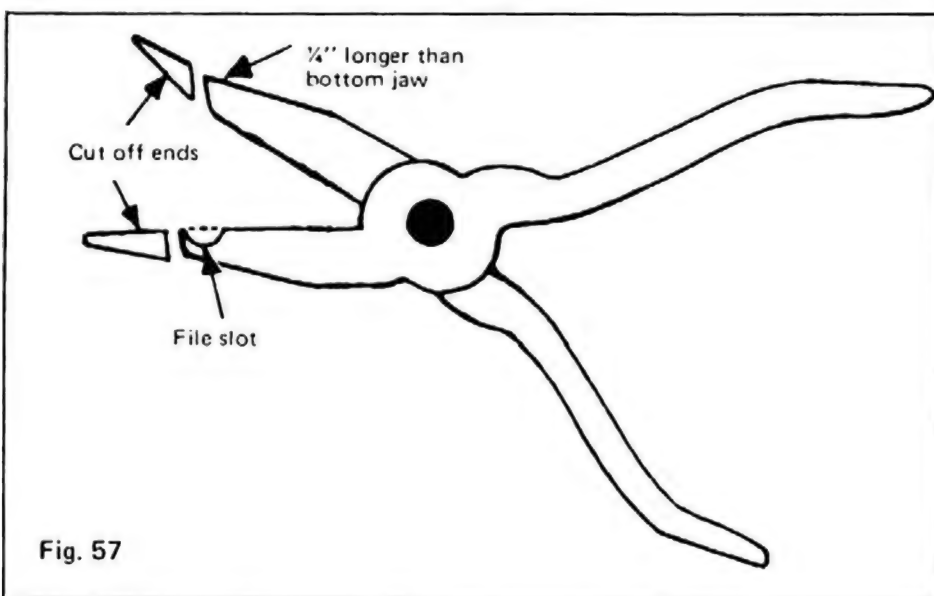
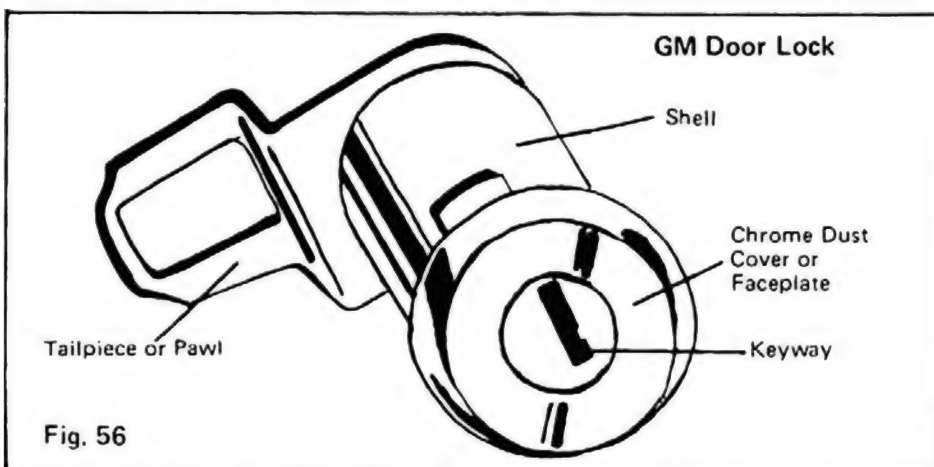
Chrysler cars having the side bar lock, have the standard pin type door lock sets, and they can be decoded in the same way any pin tumbler lock can. This is not true with the General Motors lock or American Motors door locks. General Motors have side bar locks and American Motors have "wafer" tumbler locks.

Reading The Tumblers On The GM Door Lock

The General Motors door locks differ from Chrysler and Ford in that the tumblers are inaccessible without breaking down the lock. In Ford and Chrysler, there are retainer clips on the shell of the door lock that allow easy access to the pin tumblers. On General Motors it is necessary to remove the chrome dust cover so that you can get to the plug that holds the tumblers (figure number 56).

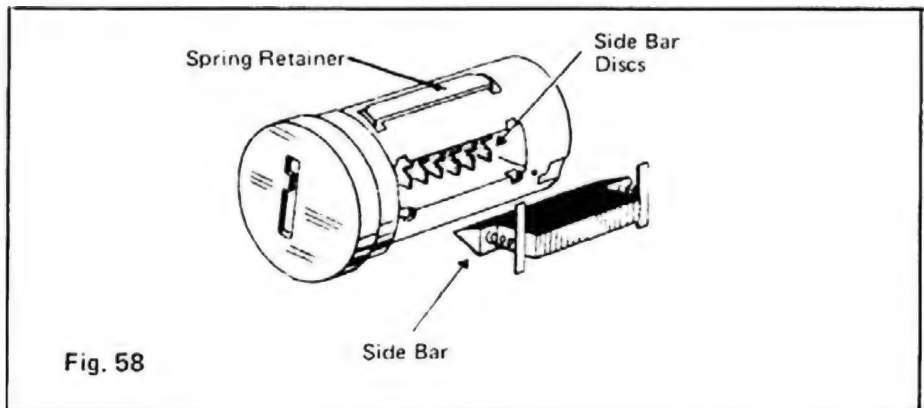
In 1974, General Motors discontinued coding the door locks to the ignitions. Instead, they coded the door locks to the trunks, making the door lock removal method obsolete.

The face cap or dust cover on the General Motors lock is pressed on, and a little effort is needed to remove them. I designed a tool out of an old pair of needle nose pliers that you could use just like a bottle cap opener. The cap will come off easily without the danger of cutting your fingers (figure number 57). Another method of removing the dust cover is by utilizing a pair of bolt or nail cutters as discussed in Chapter Two.

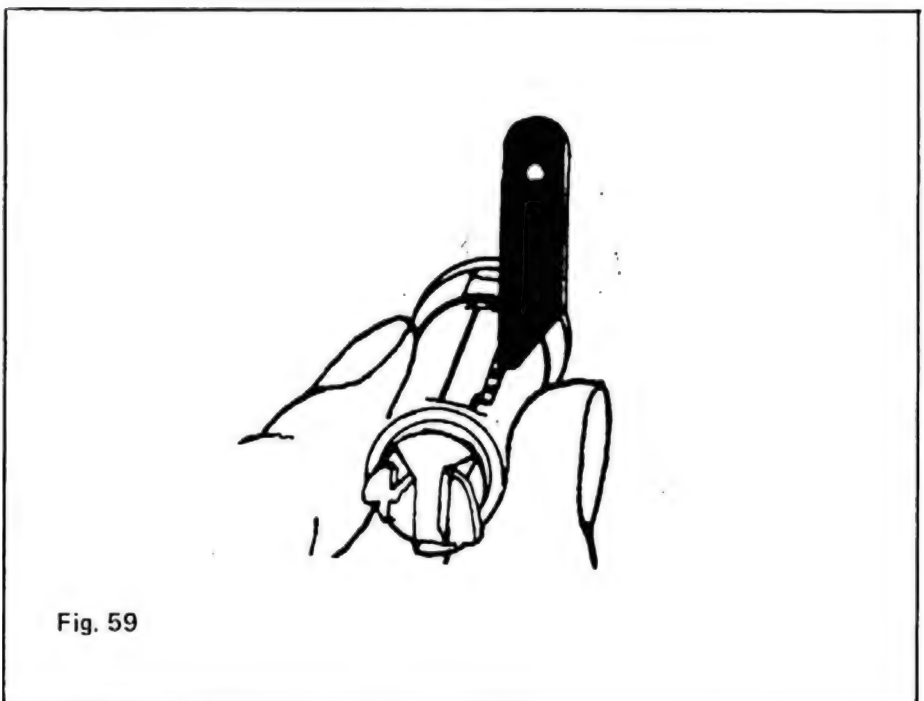


After you have removed the plug from the shell remove the side bar so that you can see the side bar discs. This is very easy to do as the side bar is only lightly staked into the plug. Take the correct blank for the particular lock, and put it into the keyway. Then look at the side bar discs. A number one cut on a General Motors lock is no cut at all, and if there are any number one cuts, the V slot will be directly in the center of the opening where the side bar once fit. The object is to cut the key until all of the V slots in the side bar discs align in the middle of that opening. If you have depth keys for each year and model of General Motors, it will be somewhat easier to figure out the cuts. If you are using a file, file slowly a little at a time until the cut is deep enough to hold the point of the V slot directly in the center of the opening made by the removal of the side bar. Check your work carefully as you file and do not go too deep. After you have succeeded with one disc perform the same filing procedure for each of the other five discs. When you have completed the work, replace the side bar. If your key is accurate the

side bar should snap into the discs and thus permit the plug to turn (figure number 58).



Another much easier method is to use a set of General Motors decoder gauges. Hand hold the plug so that your fore finger is exerting pressure on the side bar. Rake the tumblers through the keyway with a picking tool all the while keeping pressure on the side bar. It is probable that the front wafer will fall into the open position first and that the side bar will tilt inward. With further raking, the other wafers will move into the open position and the side bar will become fully depressed into the V slots of the side bar discs. It is important that you keep it there (figure numbers 59 and 60).



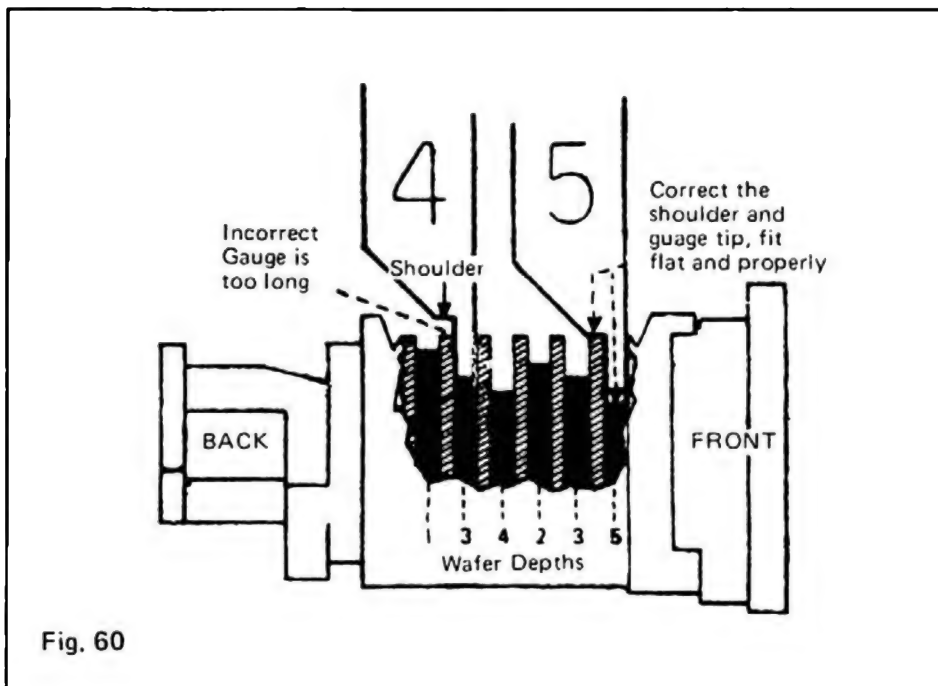




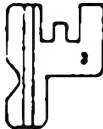
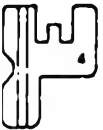


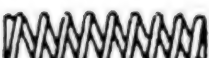
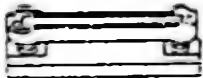


Fig. 60

Look down into the square holes at the side of the spring retainer where the wafers are visible. The wafer tops can be seen sitting at various levels. To begin decoding, start with the first space position (closest to the front of the plug). Use the longest gauge (number five) and work your way down to the shortest one, whose shoulders lie flat on the surface of the divider walls. These dividing walls are indicated in the diagram above by the diagonal lined areas.

It is important that you do not pass up the correct gauge, because the shoulder of all gauges shorter than the correct one will also lie flat and appear to be correct. Repeat the above procedure for all six tumblers and then cut a key by utilizing a file or key cutter.

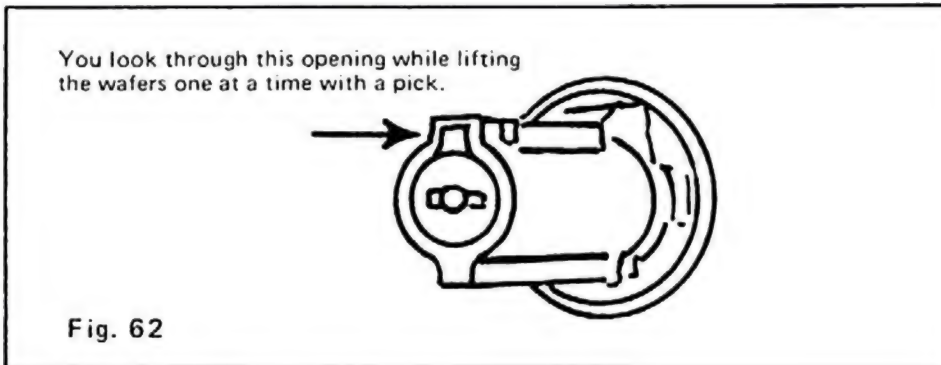


WAFER OR DISC TUMBLER SYSTEM

<p>Tumbler No. 1</p> 	<p>Tumbler No. 2</p> 	<p>Tumbler No. 3</p> 
<p>Tumbler No. 4</p> 	<p>Tumbler No. 5</p> 	<p>Tumbler Spring</p> 
<p>Tumbler Spring</p> 	<p>Side Bar Assembly</p> 	<p>Face Plate "Dust Cover"</p> 
<p>Spring Retainer</p> 		<p>Fig. 61</p>

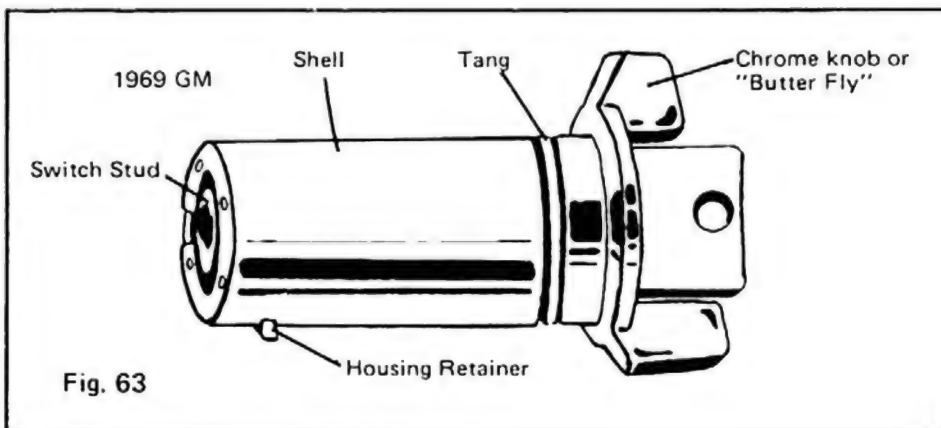
Reading The Tumblers On American Motors Door Locks

As previously discussed, some American Motors door locks are difficult to remove with any of the quick methods. It is necessary to remove the panel, and pull the lock. When the lock is out remove the tail piece (the L shaped metal piece at the base of the lock used for actuating the lock button) and look down the hole in the back. The original factory locks have the depth numbers stamped on each wafer. Using a pin light and a pick, you can raise the tumblers one at a time and read the numbers from them. Reverse the numbers, as you are reading the last cut first, cut the key by using a file or key cutter. (Figure number 62.)

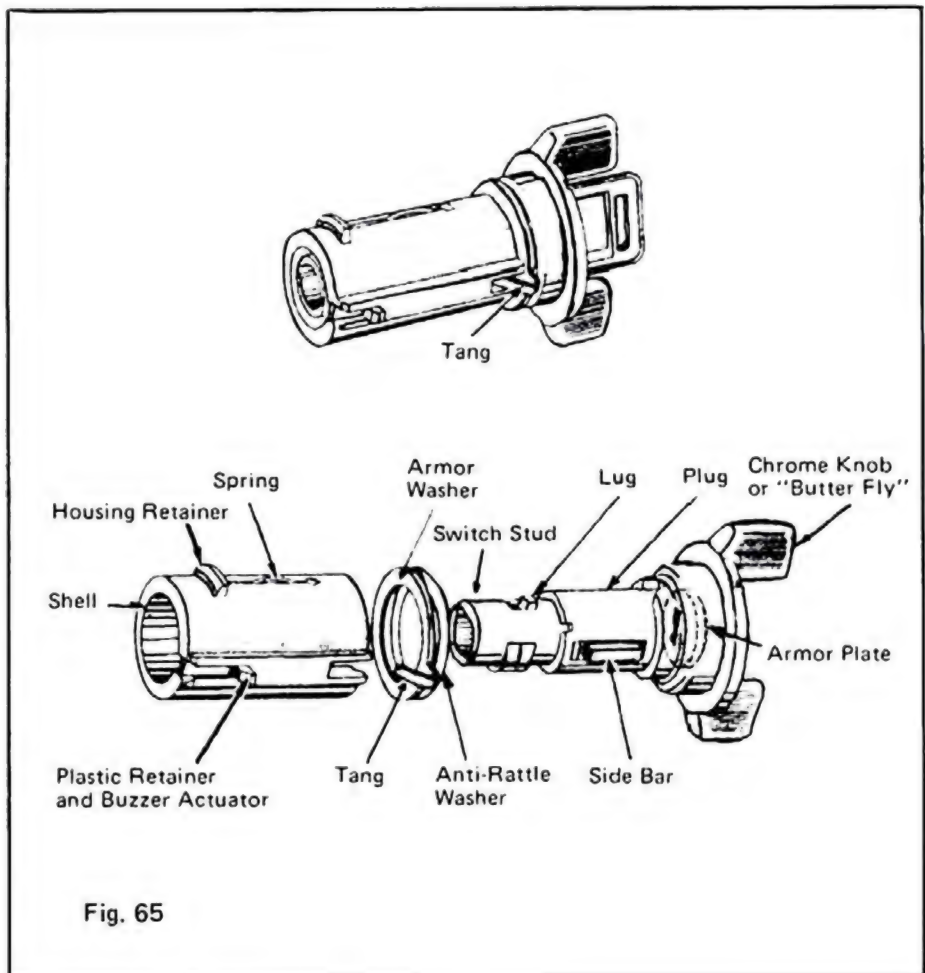
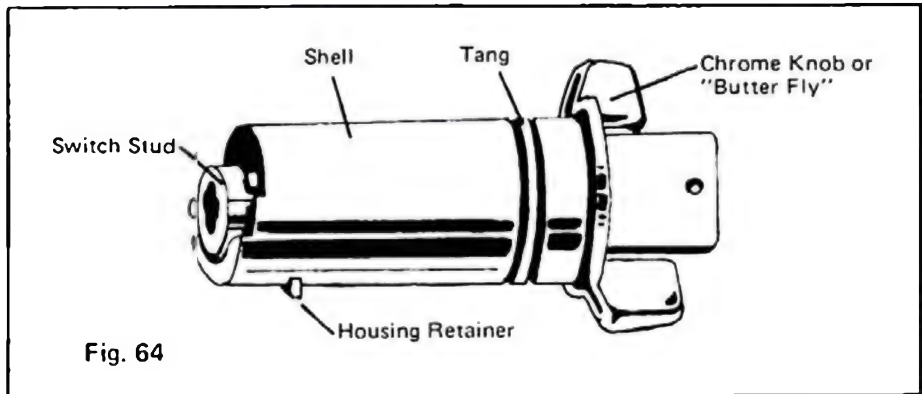


Locksmithing Techniques For General Motors, American Motors And Chrysler Tilt Wheel Ignitions

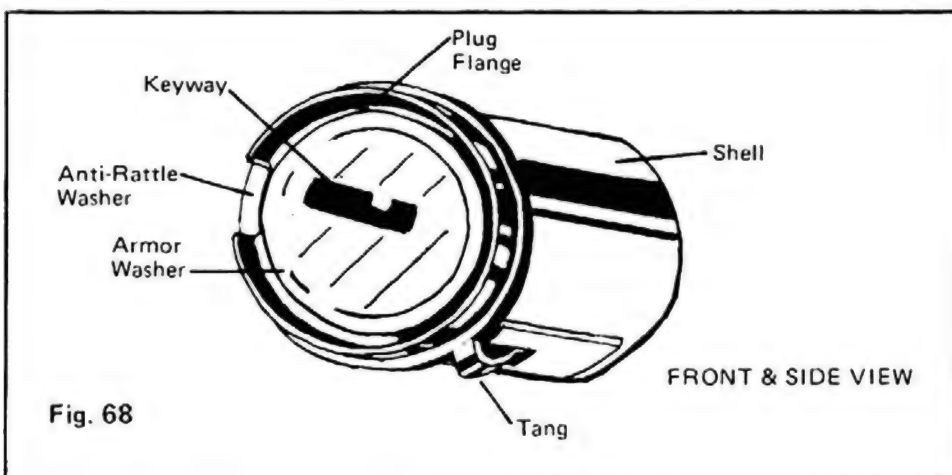
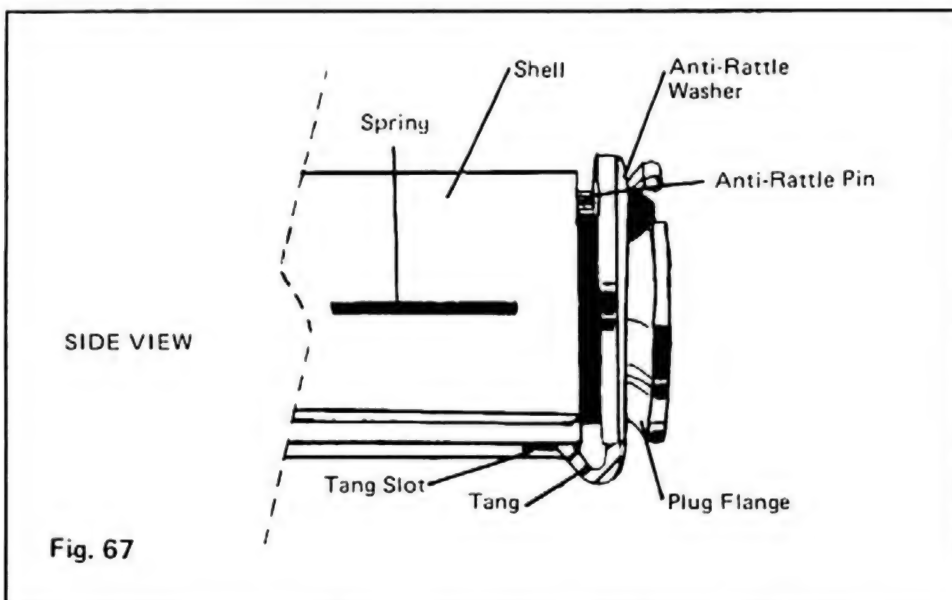
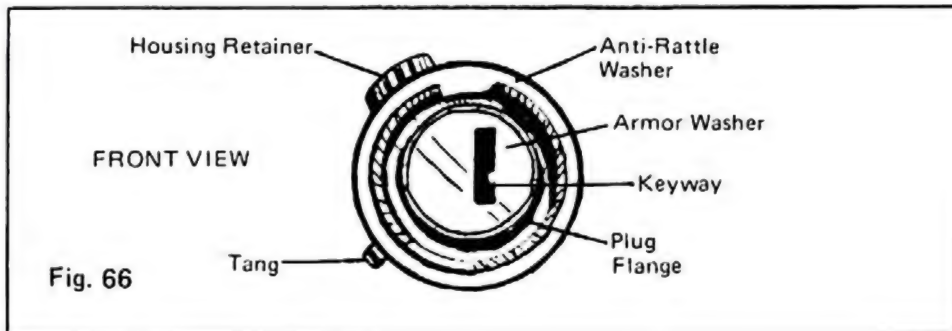
In 1969 General Motors introduced an ignition lock with three way locking. Located on the steering column, the new lock not only locked the ignition but also immobilized the steering wheel and transmission. The thought was that a would be thief might start the engine by crossing the wires, but would be prevented from stealing the car by the inability to put the vehicle into gear and turn the steering wheel. Chrysler, Ford and American Motors followed suit in 1970 with their own locked ignitions. American Motors, and Chrysler on the tilt wheel model, utilize a lock similar to the 1969 General Motors ignition lock (figure number 63).



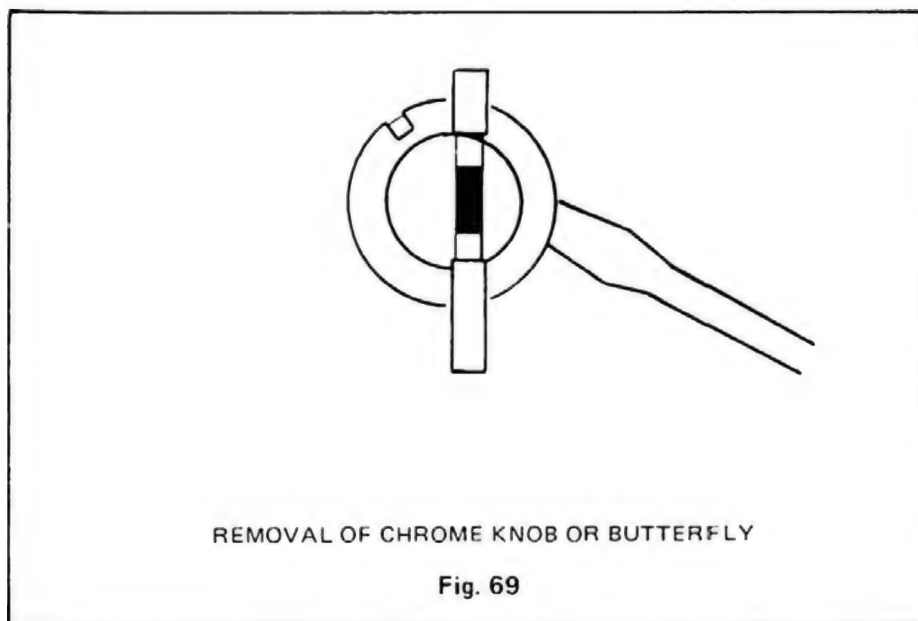
In 1970, General Motors modified their ignition lock by changing the design on the shell housing around the switch stud (figure number 64). Figure number 65 is an exploded lock view of the 1969 ignition.



In 1977 General Motors again changed their ignition lock by altering the design and diameter of the plug flange. In years previous to 1977, the plug flange diameter was approximately $7/8"$. The plug flange diameter of the 1977 and up is now $1\ 1/8"$. Figures number 66, 67, and 68 depict the plug



flange of 1969 through 1976 General Motors ignition, the 1970 and up American Motors ignition and the 1970 and up Chrysler Motors tilt-wheel ignition from various view points after removal of the chrome knob or butterfly. To remove the chrome knob or butterfly, insert a screw driver between it and the column housing to pry it off (figure number 69). After the chrome knob has been removed and the plug flange is exposed, the ignition can be extracted in several methods.

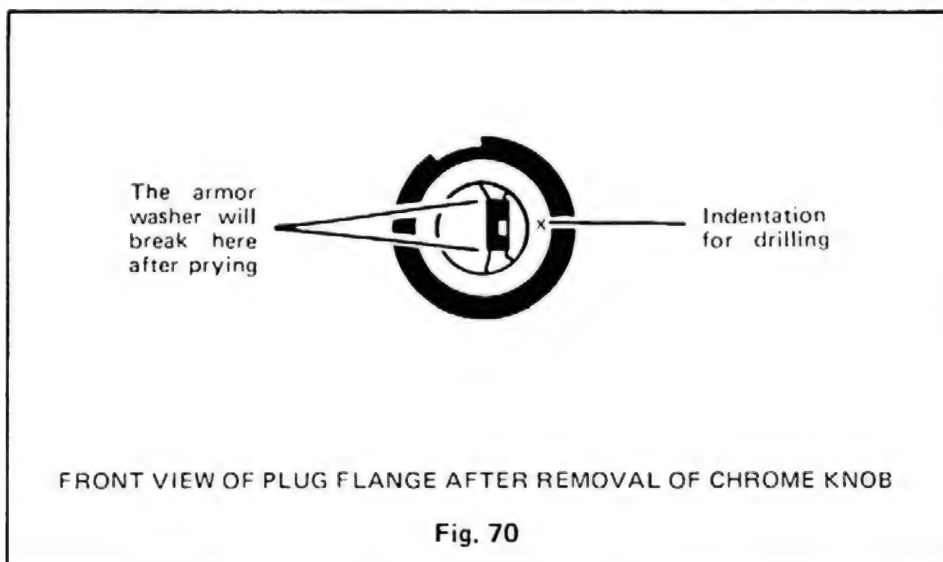


The first is by utilizing the slammer or Ford Extractor. To enable you to use these tools, it is first necessary to remove the armor keyway washer. By inserting a flat head screw driver into the keyway and prying up and down, the armor washer can be broken out in a matter of minutes. I suggest using Sears Craftsman 1/4" forged screw drivers as they will be gladly replaced by Sears if the tips break. These screw drivers come in two shaft lengths. Get both, to determine which works best for you. In prying out the armor washer with a screw driver, the object is to break the washer at it's weakest points at the top and bottom of the keyway. Do not pry side to side, as you will break the screw driver. Once the washer is broken at the top and bottom of the keyway, a slight side to side motion will break out a portion of the armor washer to the left of the keyway. With that portion of the armor washer removed, the self-tapping screw of the slammer or Ford Extractor will easily bite into the keyway allowing you to extract the ignition in the methods prescribed for those tools. An easier and more professional method of removal of the armor washer is by utilizing a drill jig and a hole saw. A 3/4" hole saw without an arbor (a guide drill) will enable you to drill away the small pot metal lip incasing the armor washer in less than a minute. It is not necessary to completely remove the pot metal lip as a slight amount of drilling will allow you to pry out the armor washer by inserting a screw driver in the keyway. To get best results, make sure that the inside hole of the drill jig is slightly larger than the 3/4" hole saw and that it is properly aligned with the armor washer. Black and Decker's cordless drill has sufficient power to

allow you to drill out the armor washer. I would suggest that you purchase two of the rechargeable battery packs for emergencies or if you plan to do a lot of drilling.

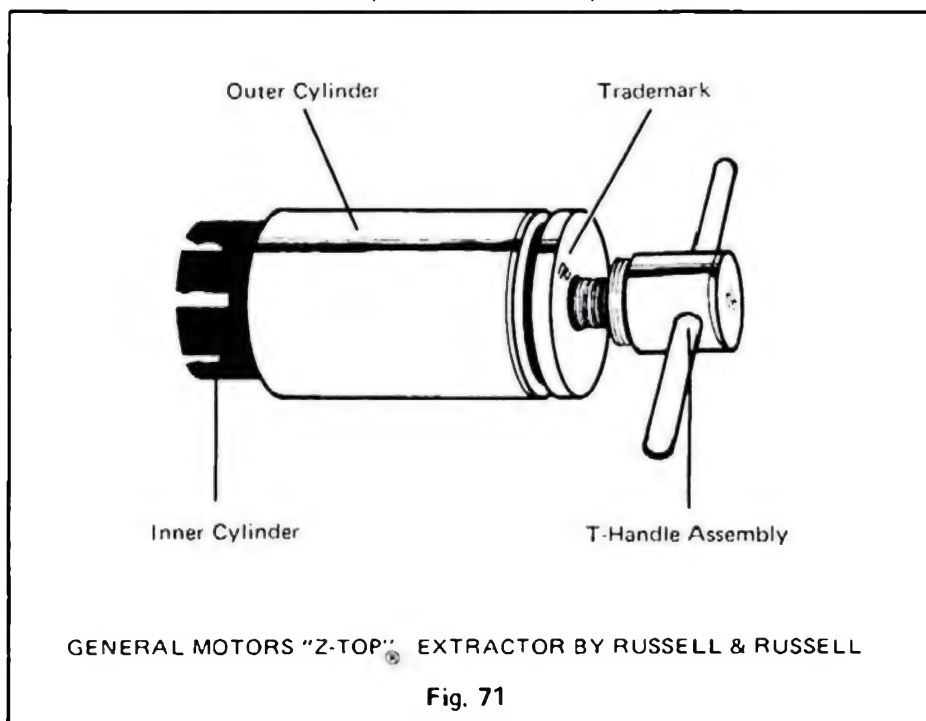
The next method is to pry away the plug flange piece by piece by placing a screw driver between it and the column housing. By using a "can opener" motion as you pry up on the plug flange, the lip of the plug flange can be removed. Once this lip is removed, you are able to remove the anti-rattle and tang washers. With the anti-rattle and tang washers removed, the tang slot (refer to figures number 66 and 67) is exposed. Screw the self-tapping screw of the slammer or Ford Extractor into the tang slot at a slight angle so that the screw bites into the plug and the shell. It is then possible to extract the lock in the usual methods.

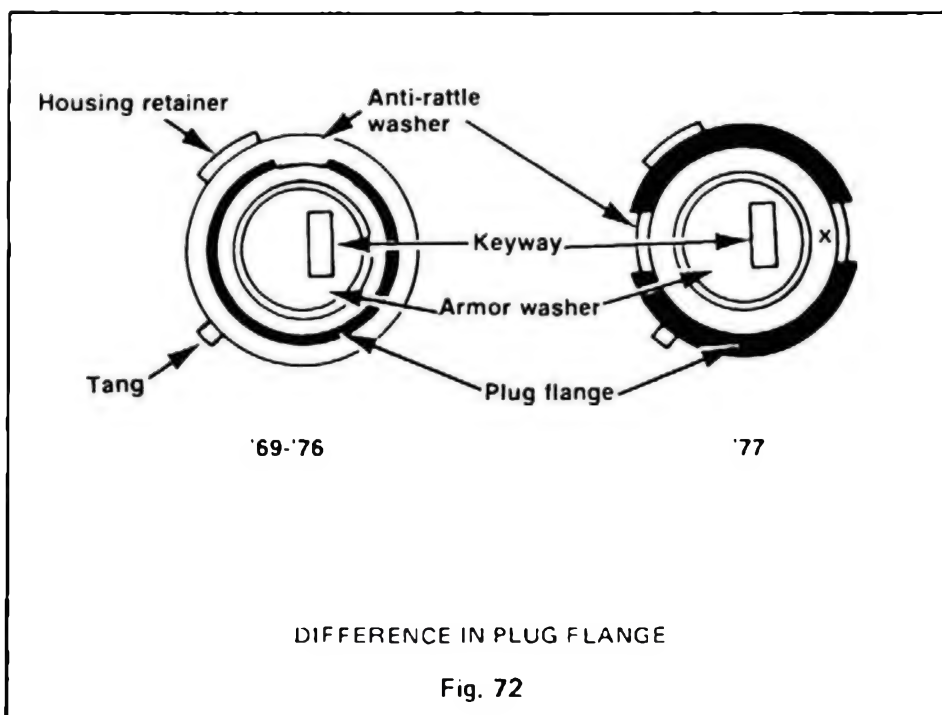
Another method is by drilling a small hole into the plug flange at a 45 degree angle. Around the armor washer there is a slight indentation. Figure number 70 depicts the approximate location of the indentation at the point marked "X" (please bare in mind that a hole can be drilled anywhere in this indentation and not specifically at the point marked "X"). Use a 3/32" carbide drill bit to drill a hole 1/2" into the plug flange and the core of the lock. By angling the drill bit 45 degrees, the drill will miss the armor washer and penetrate the core of the lock. After the hole is drilled, insert the self-tapping screw of the slammer or Ford Extractor into the hole and extract the ignition in the usual method.



Perhaps the easiest method of extracting the pre-1977 General Motors ignition, the 1970 and up American Motors ignition and the 1970 and up Chrysler tilt-wheel ignition is by utilizing the General Motors Extractor. To use this tool, the chrome knob is removed and an inner cylinder is snapped onto the plug flange. Once the inner cylinder is secure, an outer cylinder is placed around it, and the lock is ratcheted out in short order. As I have pointed out to you previously, there are several manufacturers of Extractors. Some of their products are good and others are not. The main problem with most of these Extractors is that the manufacturers do not take into account that the

diameter of the plug flange of the ignition differs from model to model. Because of this, the design of the "grabbing hooks" of the inner cylinder is critical. Most of the tools on the market use a simple 90 degree bend in the inner cylinder to form the "grabbing hooks". If you will closely examine the plug flange of the General Motors ignition, (and similar ignitions), you will notice that the flange has a slope or is angled on the back portion where the "grabbing hooks" fit. Because of this angle, those Extractors using a 90 degree hook design cause the plug flange to collapse and the ignition to stay intact in the column. Once the flange collapses, the Extractor will not work. Most manufacturers do not heat treat the inner cylinder and even if the grabbing hooks are properly designed, they wear out or break off after a while. Most of the Extractors examined have outer cylinders that are too long allowing the operator to over tighten the tool during extraction. Over tightening causes the plug flange to break, the binding of the lock in the housing, the breakage of the grabbing hooks and extraction of the core of the lock leaving the shell intact. My harping on the imperfection of my competitor's Extractors, is not for the soul purpose of pointing out the many advantages of purchasing the tools that I have designed. My specific purpose, is to point out to the consumer what to look for when purchasing a tool. Sales of my products have been affected by the imperfections of our competitor's products, making the consumer wary of utilizing any Extractor. Below is a General Motors Extractor that we developed (figure number 71) that is guaranteed to work and will be replaced if defective. The model depicted uses a T-Handle that precludes the use of a ratchet wrench. As with our other tools, we have made them as completely "fool proof" as possible, as they were developed for the repossession industry. Because many in the repossession industry practice "involuntary repossession", the failure of a tool could cause a serious problem for the reposessor.





In 1977 General Motors altered the design of the plug flange of their ignition. Figure number 72 depicts the change in design. The plug flange is wider, to impede the use of the 1970 through 1976 General Motors Extractor. General Motors did not appreciate the fact that their so called "high security" lock cylinder could be defeated so easily. General Motors also noted that there had been an increase in the sale of replacement sleeves (the shell) used by locksmiths and repossessionors to repair ignitions extracted with the General Motors Extractor. For years, General Motors had offered these sleeves to locksmiths for approximately seventy five cents apiece, and although the sales were up because of the Extractors, the sales of their ignitions dropped. Subsequently they altered the design of the plug flange and discontinued marketing replacement outer cylinder sleeves. General Motors then circulated propaganda to the effect that replacement outer sleeves would not properly align with the extracted plug and therefore, should not be used. They also advised locksmiths that the use of Extractors could cause damage to the column housing during extraction. Puzzled by why General Motors would take such serious exception to Extractors, I contacted their Steering Gear Division in Detroit. I was advised that General Motors was not concerned with the use of Extractors by those in the repossession industry, but was concerned when Extractors began to be sold to locksmiths. They explained that it is their contention that auto thieves use the cover of professional locksmiths, and that the tools would "get into the wrong hands".

To set the record straight, replacement outer cylinder sleeves have no alignment problem. If properly used, with the exception of the Chrysler Extractor, Extractors do not cause damage to the column housing. As to locksmiths being auto thieves, well I can only speculate that there may be some truth to this, but I do not feel that General Motors should have the audacity to con-

vict the whole profession for the actions of a certain few.

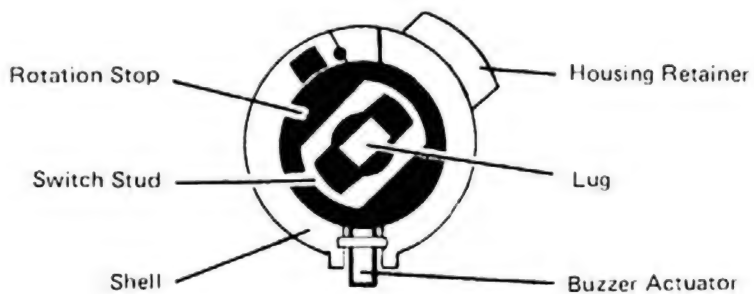
Several months after the 1977 ignition was introduced, several manufacturers introduced a 1977 General Motors Extractor. These Extractors utilize a series of small "fingers" that must be inserted one by one or two by two around the plug flange. Once these "fingers" are properly positioned, the ignition can be extracted in a similar manner as the pre-1977 Extractor. These tools will work, however, the larger flange of the 1977 and up ignition can occasionally break off leaving the ignition intact. I tried to develop a tool of similar design and found that the flange would break occasionally regardless of the design of the fingers. Because the plug flange is wider, during extraction, the flange collapses as more pressure is exerted against it during extraction. It is much like the karate expert that is able to break a 4' two by four with his hand but could not and would not attempt to break a 1' two by four without the use of a five pound hammer. Because of these problems, I have been unable to develop a tool using fingers or an inner cylinder that is a hundred percent effective in extracting the ignitions.

To extract the 1977 and up General Motors ignition, the methods described for extracting the 1969 through 1976 General Motors ignition can still be used. In other words, the armor washer can still be removed with a screw driver, the flange can be drilled and/or broken off, as previously described in this chapter. I have developed a drill jig for removal of the armor plated washer so that the Ford Extractor can be used to extract the ignition and another tool that breaks the armor plated washer out in the same fashion as a screw driver. I suggest using any of these procedures for servicing 1977 and up General Motors ignition.

Disassembly of the 1970—UP General Motors Ignition

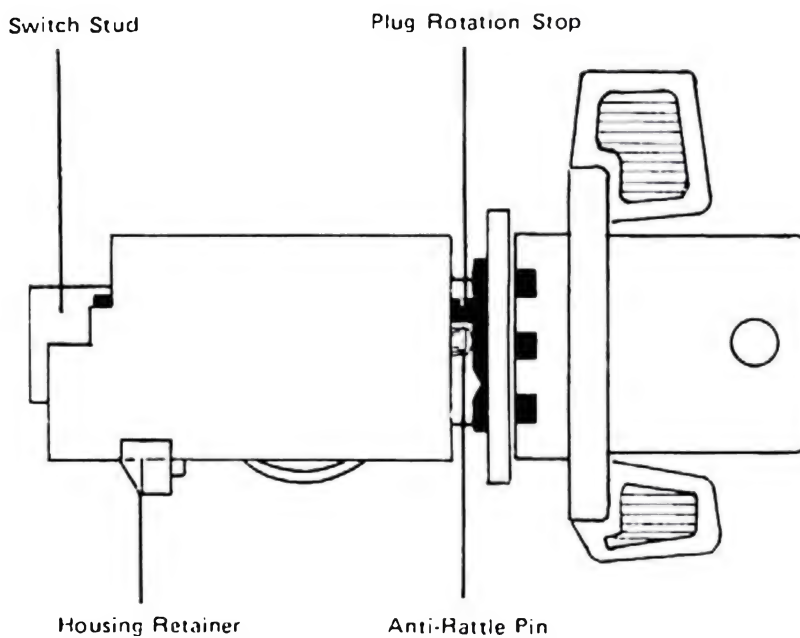
As previously mentioned, extracted ignitions can be repaired by using a replacement outer sleeve. Although General Motors no longer produces these, one major ignition manufacturer still does.

To disassemble the 1970 and up General Motors ignition, the "rotation stop" staked onto the switch stud at the base of the ignition must first be removed. To remove the "rotation stop", place a screw driver between it and the shell of the ignition and pry up. Use caution during removal so that the "rotation stop" is not broken (figure number 73). Next by using a key, turn the ignition to the "accessory" position, to the left (it is necessary to have a key for this operation, the key code is located on the shell of the extracted ignition). With a paper clip or ice pick, depress the anti-rattle pin that is closest to the housing retainer. While depressing the anti-rattle pin, continue to turn the lock to the "accessory" position so that the "plug rotation stop" travels over and past the anti-rattle pin being depressed (figure number 74). Pull back on the key and you should be able to remove the plug. Should the plug resist, it indicates that the plastic retainer—buzzer actuator is binding against the lug (figures 65 and 73). To combat this, make sure that the buzzer actuator is fully extended and if not, pull same downward with your fingers. Next use your ice pick to push up on the lug through the opening in the switch stud. The plug should then come out without any further problem. To reassemble the lock, align the side bar to the tang slot (figure number 65). Once the plug is secure in the replacement shell, reattach the "rotation stop".



REAR VIEW OF THE 1970-UP GENERAL MOTORS IGNITION

Fig. 73



SIDE VIEW OF THE 1970-UP GENERAL MOTORS IGNITION

Fig. 74

Chapter IV

General and Miscellaneous Information

Key Code Information

Key code information can be obtained by calling the title clerk at the dealership where the vehicle was originally purchased. Give the title clerk the name of the owner, the serial number and when the vehicle was purchased. The clerk should be able to pull the contract and give you the key codes.

On used cars where it is impossible for you to know who the original dealer or purchaser was, contact the Department of Motor Vehicles in title states, give them the serial number and they should be able to give you the name of the original purchaser and the original dealer. Then contact the title clerk at the original dealership as you would with a new car. This is true of all American made automobiles and trucks with the exception of Chrysler trucks as this information is not listed on the original contract.

Be sure to check the glove box for a warrenty book, the key codes are some times written on the first or second page of same.

A factory "quality control" listing sheet can be found under the springs of the driver's seat or under the carpet on the driver's side of most American made automobiles occasionally, they list the key codes on same.

American Motors

If you are on good terms with a title clerk at an American Motors dealership, it is possible to give them a serial number and have them contact the factory regarding the key codes. The key codes are cross indexed on a computer with the serial number and they can usually produce the key codes for cars manufactured as late as 1973. American Motors does not publicize this fact as the service is designed for their dealers only, so bear this in mind when trying to obtain this information. It is possible that the other major automobile manufacturers also have this same type service, but I have been unable to verify same.

Ignition key codes for American Motor's Products can be found on the shell of the ignition. Very rarely are the key codes located on the door lock. Trunk key codes can usually be found on the plug of the trunk lock. The trunk key code is usually on the plug of the glove box as are General Motors Products.

Chrysler Motors

Ignition key codes for Chrysler Motor's Products are located on the shell of the ignition and on 1970 and 1971 vehicles can be found on the passenger side door lock. Occasionally, key codes can be found on the glove box

lock of Chrysler Products. Some glove box locks for Chrysler products have only four tumblers. These are the last four tumblers from bow to tip and it is necessary to use trial and error to decode the first two cuts. Occasionally, the key codes for the trunk can be found on the shell of the trunk lock.

Ford Motors

Ignition codes for pre-1972 Ford Motor's Products can be found on the door lock on the passenger's side. Occasionally, they can be found on later year vehicles on the passenger door lock. The ignition code is rarely stamped on the extracted ignition. Trunk key codes for Ford Motor's Products are located on the back of the shell of the glove box lock. You can use a mirror to read same or it can be easily removed. Trunk key codes are usually found on the shell of the trunk lock.

General Motors

Ignition key codes for General Motor's Products from 1974 down can usually be found on either door lock or on the shell of the extracted ignition. Trunk key codes can be found on the plug of the glove box lock. When trying to remove the plug from the shell of the glove box lock, open the lid of the glove box and turn the opening knob to the left. Pull back the lock latch and pick the lock to the locked position, (usually to the left) this will put the lock retainer directly in front of you and it can then be pushed through the poke hole to allow the lock to come out.

By removing the rubber bumper in the jam of the door or by drilling or punching a hole in the jam one is usually able to see the key code for the ignition on General Motors Products 1974 and down.

Foreign

On the following foreign automobiles the key codes can be found on the shell or core of the ignition: Jaguar; Triumph; Capri; Volkswagen; Fiat; Chevrolet LUV; Ford Courier; Datsun (pre-70); Subaru; and Toyota.

The following foreign automobiles have the key codes for the door lock on the shell, pawl or core of the door lock: Opel; Porsche; Fiat; Dodge Colt; Honda; Cricket; Triumph; Mazda; Toyota and Volvo.

The key codes for the Volkswagen door lock are located on the door handle as are the codes for Renault, Capri and Mercedes Benz.

Vehicles with trunk key codes on the trunk lock are: Mazda; Dodge Colt; Toyota; Volvo; Capri; Mercedes Benz; Triumph and Opel.

It is often possible to find the key codes for the glove box, door and trunk locks on the glove box lid of Capri, Datsun and Audi vehicles.

On the hood release of the 914 Porsche, located under the dash on the driver's side, there is a cylinder which locks it. In the unlocked position only a set screw holds the cylinder plug in. When the cylinder plug is re-

moved, a key can be quite easily made from the code on same that will work on the ignition, door and trunk.

The door handle mechanism on a Volkswagen "Bug" can be easily removed by unscrewing the screws that are in the door jam under the weather stripping near the lock mechanism. The key codes are stamped on the back of the door handle.

Key codes for Mercedes Benz vehicles can be obtained by calling your local dealer. They have a cross reference book with serial numbers and key codes on all Mercedes Products.

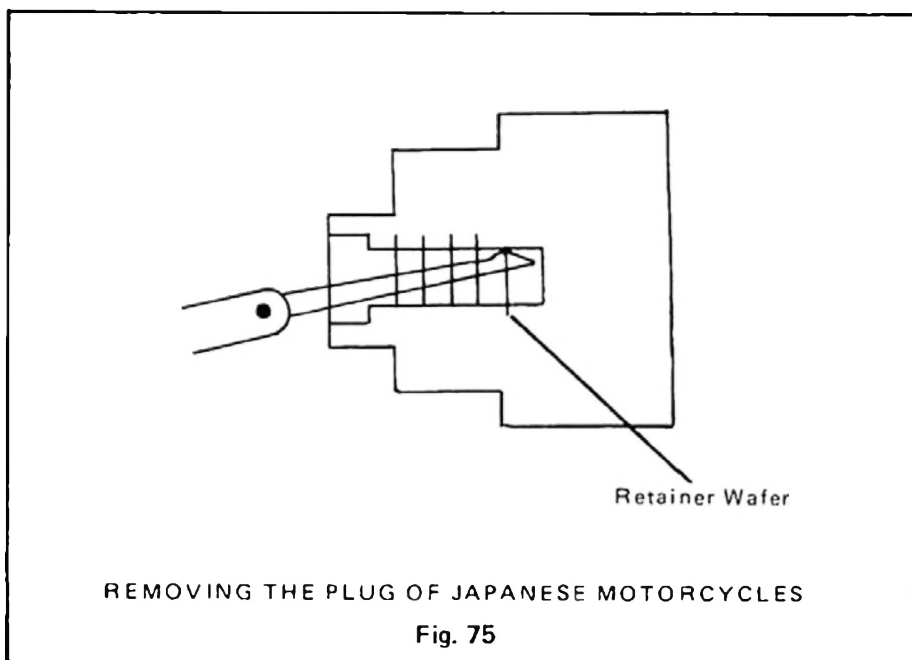
Fiats usually have key codes in warrenty books.

Gas tank locks of some foreign cars are keyed to the ignition and the code is stamped on the shell of the gas tank lock or on a paper tag on same.

Some of the information above may be inconsistant as key code locations vary from year to year and model to model, however, most of this information is correct and worth checking into.

Japanese Motorcycles

The lock cylinders in most Japanese motorcycles use five wafer tumblers. The core or plug of the lock is secured into the outer cylinder or the shell by using a retainer wafer at the bottom of the plug. To remove the core or plug, insert a diamond tipped pick into the keyway and pry up on the retainer so that the plug will be released (figure number 75). Use caution as the wafer tumblers are loose and can be easily lost. Most Japanese motorcycles also have the key codes stamped on the face plate of the ignition.



BERSERKER

BOOKS

